



Università degli studi  
“G. d’Annunzio”

Piano di Azioni per la  
Digitalizzazione dei Processi e  
dei Servizi di Ateneo (PADPSA)

***Quinquennio 2021-2023/2024-2025***

## Sommario

1.	PREMESSA.....	3
2.	RISULTATI CONSEGUITI NEL PERIODO 2020-2021 E NEL PRIMO SEMESTRE 2022.....	4
3	AZIONI PROGRAMMATE NEL SECONDO SEMESTRE 2022 E NELL'ANNO 2023-2025 .....	30
3.1	SERVIZI .....	30
3.2	DATI e INTEROPERABILITA' .....	31
3.3	PIATTAFORME.....	32
3.4	SICUREZZA INFORMATICA E MODALITA' ATTUATIVE DEL LAVORO AGILE .....	32
3.5	STUDIO DELLA POSSIBILITA' DI ADOTTARE PIATTAFORME DI INTELLIGENZA ARTIFICIALE (IA)....	33

## 1. PREMESSA

Il **Piano di Azioni per la Digitalizzazione dei Processi e dei Servizi di Ateneo (PADPSA)**, elaborato su base triennale, definisce il tragitto che l'Ateneo intende perseguire per conseguire una molteplicità di obiettivi finalizzati alla digitalizzazione dei processi e ad una maggiore innovazione tecnologica che possa consentire lo snellimento di procedure di lavoro nell'Ateneo. In particolare sono individuati dei progetti, alcuni dei quali iniziati nel 2020, che verranno sviluppati nel prossimo triennio in relazione alla digitalizzazione di servizi e l'ottimizzazione e razionalizzazione dei processi. Gli obiettivi prefissati, come declinati nel Piano, mirano all'accrescimento del livello di digitalizzazione dei processi ed in particolar modo alla riduzione dei costi di esercizio dell'Ateneo, obiettivo da realizzarsi anche attraverso un percorso di evoluzione e di adattamento alle mutate esigenze dovute all'emergenza epidemiologica da Covid-19. La pandemia ha indubbiamente generato una metamorfosi epocale nelle università italiane, imponendo in maniera precipitosa il cambiamento del paradigma delle modalità di erogazione dei percorsi formativi, delle modalità di verifica del livello di apprendimento da parte della popolazione studentesca e finanche dei servizi che l'Ateneo offre all'intera comunità accademica. Il presente documento, nell'ottica di una programmazione triennale, vuole assumere la connotazione un caposaldo operativo su cui basare le innovazioni tecnologiche da conseguire entro il 2023, essendo le stesse considerate come l'autentico volano volano per la conduzione del processo di trasformazione digitale finalizzato al miglioramento dei livelli di servizio offerti dalla Pubblica Amministrazione (PA).

Il Piano Triennale per l'informatica della Pubblica Amministrazione (di seguito Piano Triennale) è uno strumento essenziale per promuovere la trasformazione digitale del Paese e, in particolare, quella della Pubblica Amministrazione italiana. I cambiamenti da attuare saranno accompagnati da nuove normative e nuove opportunità che aiuteranno il Paese a proseguire nella direzione della trasformazione digitale già iniziata. Il Piano Triennale si pone infatti come sintesi tra le varie linee di trasformazione digitale della PA. L'aggiornamento 2021-2023 del Piano Triennale 2020-2022, in continuità con la precedente edizione, consolida l'attenzione sulla realizzazione delle azioni previste e sul monitoraggio dei risultati raggiunti nel raggiungimento degli obiettivi predefiniti, di seguito evidenziati:

- favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della PA che costituisce il motore di sviluppo per l'intero Paese;
- promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale.
- contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

I principi guida, su cui si basa il Piano Triennale sono:

- *Digital & mobile first* (digitale e mobile come prima opzione). Le Pubbliche Amministrazioni (PA) devono realizzare servizi primariamente digitali;
- *Digital identity only* (accesso esclusivo mediante identità digitale). Le PA devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;
- *Cloud first* (cloud come prima opzione). Le PA, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma *cloud*, tenendo conto della necessità di prevenire il rischio di *lock-in*;
- *Servizi inclusivi e accessibili*. Le PA devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- *Dati pubblici, un bene comune*. Il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;

- *Interoperabile by design*. I servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- *Sicurezza e privacy by design*. I servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- *Eser-centric, data driven e agile*. Le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.
- *Once only*. Le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;
- *Transfrontaliero by design* (concepito come transfrontaliero). Le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- *Open source*. Le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice sorgente aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

Nel decreto-legge n. 76/2020 (come convertito dalla Legge n. 120/2020), recante misure urgenti per la semplificazione e l'innovazione digitale, sono previste azioni volte a promuovere e a valorizzare l'informatizzazione della Pubblica Amministrazione: una su tutte la promozione dell'uso del sistema di identità digitale ai fini non solo dell'identificazione degli utenti, ma per consentire l'accesso ai servizi on line previa identificazione attraverso il sistema Sistema Pubblico di Identità Digitale (SPID) e la Carta di Identità Elettronica (CIE). L'innovazione e la digitalizzazione nel periodo post Covid-19 sarà focalizzata, in particolare, sulle modalità di svolgimento del lavoro agile nella PA. Quest'ultima, chiamata ad affrontare un cambiamento culturale epocale, mira alla reingegnerizzazione di tutti i processi lavorativi finora strutturati sul modello *present based* o *office based*. Sulla base di quanto evidenziato, nel presente documento sono di seguito riportate le risultanze delle azioni condotte nel periodo 2020-2021 e primo semestre 2022, e quelle condotte nel primo semestre 2022 e programmate per il 2023.

## 2. RISULTATI CONSEGUITI NEL PERIODO 2020-2021 E NEL PRIMO SEMESTRE 2022

La gestione per processi rappresenta uno dei pilastri fondamentali per la gestione dell'organizzazione improntata alla qualità, all'efficienza, al miglioramento continuo e al raggiungimento di un maggiore efficientamento dell'intera infrastruttura amministrativa di un'organizzazione. Sin dal 2020, nell'Ateneo, l'azione è stata focalizzata sulla riorganizzazione della comunicazione, della didattica, della gestione degli studenti e dei servizi loro offerti, e tutti i servizi erogati in modalità DaD (Didattica a Distanza). Durante l'emergenza sanitaria lo svolgimento delle prestazioni lavorative a distanza ha imposto un maggiore utilizzo delle tecnologie informatiche come strumento di lavoro di riferimento. Le piattaforme digitali, le applicazioni software e i device di tipo "mobile" hanno prodotto una sostanziale modificazione delle attività lavorative del personale dell'Ateneo, facilitando la comunicazione le modalità di gestione delle relazioni e finanche l'ottimizzazione della condivisione, la memorizzazione e l'archiviazione dei documenti. Applicazioni software come Microsoft Teams, hanno consentito di sfruttare le funzionalità degli strumenti di "collaboration" come spazi di lavoro condivisi, spazi in cui creare le cosiddette "cartelle condivise", creare gruppi/team specifici, chat e video chiamate, gestione riunioni online. I progetti che hanno impegnato l'Ateneo nel corso del periodo 2020-2021 e primo semestre 2022, riferibili ad alcune delle linee di azione del Piano Triennale, sono rispettivamente:

- ☑ la migrazione degli applicativi e dei sistemi informatici per infrastrutture e servizi cloud qualificati;
- l'accessibilità dei servizi informatici (portali web e app) dell'Ateneo;
- l'adesione al Sistema Pubblico di Identità Digitale (SPID), alla Carta di Identità Digitale (CIE);
- l'adesione al sistema di IDEntity Management per l'accesso federato (IDEM);
- l'attivazione servizi ERASMUS+ per gli studenti;

- l'aggiornamento dei formati trattati dal sistema di conservazione di Ateneo sulla base delle nuove Linee Guida dell'agenzia per l'Italia Digitale (AgID).
- l'adozione della firma digitale per il personale dell'Ateneo integrato con il programma di gestione documentale Titulus del Cineca.

Per quanto concerne il secondo semestre 2022 e l'anno 2023, le azioni previste sono:

- il rafforzamento delle competenze digitali del personale dell'Ateneo onde favorire una maggiore inclusione digitale;
- la definizione, all'interno dei piani di formazione del personale, di interventi sulle tematiche di Cyber Security Awareness;
- l'adeguamento delle infrastrutture digitali dell'Ateneo alle Misure minime di sicurezza ICT per le pubbliche amministrazioni<sup>1</sup> aggiornate;
- ☒ la reingegnerizzazione del portale web di Ateneo.

Di seguito sono elencate le azioni condotte dell'Ateneo nel periodo 2020-2021 e primo semestre 2022 e sono riconducibili ad alcuni degli "Obiettivi e risultati attesi" evidenziati nel Piano Triennale.

**Punto OB.1.2 (Migliorare l'esperienza d'uso e l'accessibilità dei servizi) – Linea d'azione R.A.1.2c - Incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici.**

**Periodo: 2020-2021**

**Azione dell'Ente: Analisi dell'accessibilità dei sistemi informatici.** Per accessibilità si intende la capacità dei sistemi informatici di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di forme di disabilità necessitano di tecnologie assistive o particolari configurazioni degli applicativi. La legge di riferimento per l'Accessibilità digitale è la n.4 del 9 gennaio 2004 che ha attribuito all'Agenzia per l'Italia Digitale (AGID) una varietà di compiti, tra cui:

- a) vigilare sull'attuazione della stessa Legge;
- b) fornire assistenza alla Pubblica Amministrazione per l'applicazione della normativa vigente;
- c) emanare regole tecniche, circolari e linee guida in materia di accessibilità degli strumenti informatici;
- d) monitorare i siti web e le applicazioni mobili della Pubblica Amministrazione;
- e) relazionare periodicamente la Commissione Europea sugli esiti di monitoraggio;
- f) divulgare i temi dell'accessibilità nella Pubblica Amministrazione;

Nel 2018, con Decreto legislativo n.106 che modifica e aggiorna la Legge n.4/2004, l'Italia ha recepito la Direttiva UE 2016/2102, volta a migliorare l'accessibilità dei siti web e delle app mobile nel settore pubblico di ciascun paese membro dell'UE. A tal proposito, nel rispetto di tale Direttiva Europea, l'AGID ha emanato il documento "Linee Guida sull'Accessibilità degli strumenti informatici" ([https://trasparenza.agid.gov.it/archivio19\\_regolamenti\\_0\\_5382.html](https://trasparenza.agid.gov.it/archivio19_regolamenti_0_5382.html)) e FAQ (<https://www.agid.gov.it/it/domande-frequenti/accessibilit%C3%A0>), in vigore dal 10 gennaio 2020, che indirizza la Pubblica Amministrazione all'erogazione di servizi maggiormente accessibili. Una delle novità di maggior rilievo per le amministrazioni riguarda l'obbligo di pubblicazione di una "Dichiarazione di accessibilità" in cui le stesse amministrazioni indicheranno lo stato di conformità di ciascun sito e applicazione "mobile" ai requisiti di accessibilità. La Dichiarazione contiene una procedura, chiamata "Meccanismo di feedback", a disposizione degli utenti che volessero segnalare ulteriori problemi di

<sup>1</sup> [https://www.agid.gov.it/sites/default/files/repository\\_files/allegato\\_4\\_-\\_linee\\_guida\\_per\\_la\\_modellazione\\_delle\\_minacce-dlt.pdf](https://www.agid.gov.it/sites/default/files/repository_files/allegato_4_-_linee_guida_per_la_modellazione_delle_minacce-dlt.pdf)

inaccessibilità. L'AGID è chiamata a effettuare il monitoraggio dei siti web e delle applicazioni mobili e a relazionare periodicamente alla Commissione Europea. L'attività di verifica di conformità si basa sull'analisi dei contenuti dei siti web di Ateneo, comprendendo le informazioni testuali e non testuali, documenti e moduli scaricabili e forme di interazione bidirezionale, come ad esempio il trattamento di moduli digitali e il completamento dei processi di autenticazione, identificazione e pagamento, così come previsto dal capitolo "9 Web" dalla norma UNI EN 301549:2018. Nella valutazione, i siti web vengono valutati come singole pagine web. Le applicazioni web e quelle web mobili sono comprese nella definizione di pagina web che è abbastanza ampia e contempla tutti i tipi di contenuto web. 3.2.1.. La verifica tecnica di conformità delle pagine web è realizzabile, ove le condizioni siano applicabili, secondo quanto previsto nel prospetto A.1 presente all'interno dell'Appendice A della norma UNI EN 301549:2018. La verifica di conformità è relativa alle pagine web che includono:

- a. documenti in forma di pagine web;
- b. documenti che sono incorporati nelle pagine web e che sono utilizzati nella rappresentazione o che sono destinati a essere rappresentati insieme alla pagina web in cui sono incorporati;
- c. software che è una pagina web;
- d. software incorporato nelle pagine web e utilizzato nella rappresentazione o destinato alla rappresentazione insieme alla pagina web in cui è incorporato.

Oltre a quanto sopra esposto, il riferimento tecnico della norma UNI EN 301549:2018 per i documenti inseriti all'interno delle pagine web (inclusi i documenti e moduli scaricabili) è il capitolo "10 Documenti non web". Il Responsabile della Transizione Digitale è tenuto a compilare online sul sito AGID una "Dichiarazione di accessibilità" entro il 23 settembre 2020. Lo stato di conformità da compilare nella "Dichiarazione di Accessibilità" per ciascun sito web (*Conforme/Parzialmente Conforme/Non Conforme*) deve essere dimostrato tramite un report di valutazione da conservare ed esibire solo su richiesta dell'AGID. Le Linee Guida AGID indicano di realizzare un report per ogni istanza di sito web (portale istituzionale, siti federati, ed aree ad accesso riservato). Nel caso dei siti realizzati a partire da un modello (es. dipartimenti, scuole, ecc), gli errori sulle funzionalità potranno essere comuni, mentre quelli redazionali (es. mancanza del testo alternativo alle immagini, tabelle senza gli opportuni tag) potranno variare da istanza a istanza. In funzione di quanto evidenziato, nel periodo di riferimento, è stata condotta un'attività di analisi sulla struttura e sui contenuti dei portali web di Ateneo seguito evidenziati:

- Portale di Ateneo ([www.unich.it](http://www.unich.it));
- Portale di Ateneo – in inglese ([en.unich.it](http://en.unich.it));
- Portale del Dipartimento di Scienze Filosofiche, Pedagogiche ed Economico-Quantitative ([www.disfipeq.unich.it](http://www.disfipeq.unich.it));
- Portale del Dipartimento di Scienze Geologiche ([www.scienzegeologiche.unich.it](http://www.scienzegeologiche.unich.it));
- Portale della Scuola Superiore dell'Ateneo ([www.scuolasuperiore.unich.it](http://www.scuolasuperiore.unich.it));
- Portale del Dipartimento di Economia ([www.dec.unich.it](http://www.dec.unich.it));
- Portale del Dipartimento di Economia Aziendale ([www.dea.unich.it](http://www.dea.unich.it));
- Portale del Dipartimento di Scienze Giuridiche e Sociali ([www.dsgs.unich.it](http://www.dsgs.unich.it));
- Portale della Scuola di Economia ([scuolaeconomia.unich.it](http://scuolaeconomia.unich.it));
- Portale del Dipartimento di Neuroscienze e Imaging ([www.dnisc.unich.it](http://www.dnisc.unich.it));
- Portali del Dipartimento di Architettura ([www.architettura.unich.it](http://www.architettura.unich.it) e [dda.unich.it](http://dda.unich.it));
- Portale di Medicina ([www.med.unich.it](http://www.med.unich.it))

Si sottolinea che l'attività condotta è fondamentale per l'invio della "Dichiarazione di Accessibilità" all'Agenzia per l'Italia Digitale (AGID). Si evidenzia altresì che lo stato di conformità da compilare nella "Dichiarazione di Accessibilità" per ciascun sito deve essere ricavato da una delle seguenti analisi:

- a) un'autovalutazione effettuata direttamente da soggetto erogatore;
- b) una valutazione effettuata da terzi;

- c) una valutazione effettuata con il “Modello di autovalutazione”, reso disponibile online da AGID e riportato nell’Allegato 2 delle Linee Guida AGID.

Per quanto concerne l’Ateneo, l’attività di analisi è stata condotta dal sottoscritto in collaborazione con il CINECA cui è affidata la gestione del portale istituzionale di Ateneo e di buona parte dei siti federati.

**Azione dell’Ente: Produzione e pubblicazione dei report di Accessibilità dei sistemi informatici sul portale dell’Agenzia per l’Italia Digitale (AGID) e sul portale istituzionale di Ateneo.** Con riferimento al punto precedente, al termine dell’attività di analisi condotta sull’accessibilità di tutti i portali web di Ateneo censiti, sono stati prodotti e pubblicati sul portale dell’AGID, e successivamente su quello istituzionale di Ateneo, i report di accessibilità relativi ai siti web attivi e di seguito elencati:

1. Portale istituzionale di Ateneo (<http://www.unich.it>)
2. Portale in lingua inglese dell’Ateneo (<http://en.unich.it>)
3. Dipartimento di Architettura (<https://www.dda.unich.it/>)
4. Dipartimenti di Farmacia (<https://www.farmacia.unich.it/>)
5. Dipartimento di Ingegneria e Geologia (<https://www.ingeo.unich.it>)
6. Dipartimento di Lettere, Arti e Scienze Sociali ([www.dilass.unich.it](http://www.dilass.unich.it))
7. Dipartimento di Lingue, Letterature e Culture Moderne (<https://www.lingue.unich.it/>)
8. Dipartimento di Medicina e Scienze dell’Invecchiamento (<https://www.dmsi.unich.it>)
9. Dipartimento di Scienze Filosofiche, Pedagogiche ed Economico-Quantitative (<https://www.disfipeq.unich.it>)
10. Dipartimento di Scienze Mediche, Orali e Biotecnologiche (<https://www.dismob.unich.it>)
11. Dipartimenti di Scienze Psicologiche, della Salute e del Territorio (<https://www.disputer.unich.it>)
12. Corso di Studio Ingegneria delle Costruzioni (<https://www.ingegneriadellecostruzioni.unich.it>)
13. Orientamento & Placement (<https://orientamento.unich.it>)
14. Centro Linguistico di Ateneo (<https://cla.unich.it/>)
15. Museo Universitario (<https://www.museo.unich.it/>)
16. Presidio della Qualità di Ateneo (<https://pqa.unich.it/>)
17. CRUST – Interuniversity Center (<https://www.crust.unich.it/>)
18. Corso di studi in Scienze Geologiche (<https://www.scienzegeologiche.unich.it/it>)
19. Nucleo di valutazione (<https://nucleo.unich.it/>)
20. Area della Pianificazione e Controllo (<https://www.apc.unich.it/>)
21. CAST - Center for Advanced Studies and Technology (<https://www.cast.unich.it/>)
22. Quality Assurance (<http://www.unichqa.prod.cineca.it>)
23. Coordinamento Didattica, Ricerca e Terza Missione (<https://st24-unichd7cl2.prod.cineca.it/>)
24. Corso di Laurea in Ingegneria Biomedica (<https://st02-unich-d7cl2.prod.cineca.it/>)
25. Scuola Superiore “G. d’Annunzio” (<http://www.scuolasuperiore.unich.it>)
26. Scuola di Economia (<http://www.scuoladieconomia.it>)
27. Scuola di Medicina e Scienze della Salute (<http://www.med.unich.it>)
28. Dipartimento di Neuroscienze e Imaging (<http://www.dnisc.unich.it>)
29. Dipartimento di Architettura (<http://www.architettura.unich.it>)
30. Dipartimento di Scienze Giuridiche e Sociali (<http://www.dsgrs.unich.it>)
31. Dipartimento di Economia Aziendale (<http://www.dea.unich.it>)
32. Dipartimento di Economia (<http://www.dec.unich.it>)

Va evidenziato che, sulla base di un ulteriore approfondimento dell'analisi dei portali web esistenti in Ateneo, è stato rilevato un numero maggiore degli stessi pari a n.20, elevando quindi il numero da 12 (siti web identificati nell'analisi iniziale) a 32. Sulla base di tale rinvenimento, è stata condotta una nuova attività di analisi degli ulteriori portali web, esaminandone analiticamente i contenuti per verificare la rispondenza con i livelli di conformità fissati dall'AGID. L'attività di analisi e valutazione è stata effettuata con una metodologia di verifica a campione secondo il metodo di monitoraggio approfondito illustrato nelle Linee Guida di accessibilità AGID al Capitolo 5. In particolare si è proceduto con la selezione un campione di pagine e di documenti secondo i seguenti criteri:

1. la home page;
2. la pagina di autenticazione;
3. la mappa del sito;
4. la pagina dei contatti;
5. la pagina della guida e le pagine contenenti le informazioni legali;
6. almeno una pagina pertinente per ciascuna tipologia di servizio offerto dal sito web o dall'applicazione mobile e per qualsiasi altro utilizzo principale previsto, compresa la funzionalità di ricerca;
7. le pagine contenenti la dichiarazione di accessibilità e le pagine con il meccanismo di feedback;
8. esempi di pagine dall'apparenza sostanzialmente distinta o che presentano una tipologia di contenuti diversa;
9. almeno un documento pertinente scaricabile, dove applicabile, per ciascun tipo di servizio offerto dal sito web e per qualsiasi altro utilizzo principale previsto;
10. se una pagina fa parte di una serie di pagine che presentano un processo oppure una sequenza di passi da completare allo scopo di portare a termine un'attività occorre considerare tutte le pagine Web relative al processo o sequenza;
11. un numero di pagine selezionate a caso pari ad almeno il 10% del campione definito ai precedenti punti (1-10)

Nel periodo 2020-2021, così come avverrà per gli anni successivi, si è proceduto, per ogni singolo anno, alla pubblicazione dei report di accessibilità di tutti i siti web censiti sul portale dell'Agenzia per l'Italia Digitale (AGID), rispettando, pertanto, le scadenze fissate per settembre 2020 e 2021. Successivamente sono stati pubblicati sulla pagina "Accessibilità" del portale di Ateneo (<https://www.unich.it/accessibilita>), i links relativi ai report di accessibilità dei siti web di Ateneo pubblicati sul portale dell'AGID.

**Punto OB.4.1 (Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle Amministrazioni locali migrandone gli applicativi on-premise (data center Gruppo B) verso infrastrutture e servizi cloud qualificati).**

**Periodo: 2020-2022**

**Azioni dell'Ente: Proiezione dell'intera infrastruttura informatica verso infrastrutture e servizi cloud avanzati.** Sulla base del cambio di paradigma da "infrastruttura on-premise" a "infrastruttura cloud", esigenza manifestata dal Consiglio di Amministrazione dell'Ateneo (delibera del 10.04.2018 – Odg 04/06) in cui veniva evidenziata l'esigenza di "....proiettare l'intera infrastruttura informatica dell'Ateneo su sistemi informativi e di comunicazione [...] particolarmente avanzati (ad es. Cloud computing)..." e manifestata come indirizzo anche dall'Agenzia per l'Italia Digitale (AGID) nel "Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021", per qualificare i servizi e le infrastrutture informatiche delle PA secondo specifici parametri di sicurezza e affidabilità nel rispetto dei seguenti principi, sono state condotte le seguenti attività:

- a) *Identificazione e analisi delle piattaforme di tipo Virtual Machine (VM) presenti nel Data Center di Ateneo (Palazzo del Rettorato – Livello 1, Area Informatica).* L'attività di analisi delle VM è stata

condotta sulla base dei dati forniti dal Settore Reti, Sistemi e Progettazione Web. È stata rilevata la presenza di n. 32 Virtual Machine “attive” che erogano servizi di diversa tipologia (web server, file server, mail server, etc.). In funzione di un’attenta e dettagliata analisi condotta sulle motivazioni che hanno dato origine, nel decennio precedente, alle richieste di attivazione di tali sistemi, e sulla base della verifica della effettiva utilità e fruibilità delle suddette piattaforme (condotta finanche con un contatto telefonico avvenuto con ogni singolo referente delle VM attive nel Data Center) è stato rilevato che almeno n. 11 VM (altre 5 sono ancora in fase di analisi) sono da dismettere per motivazioni diverse (la piattaforma non viene più utilizzata, i referenti non sono più in servizio in università, le applicazioni sono state trasferite su altri sistemi, etc.). E’ stato altresì rilevato che diverse VM non venivano più utilizzate da anni, anche se la loro piena funzionalità è stata garantita quotidianamente dal Settore Reti, Sistemi e Progettazione Web. Ciò ha indubbiamente prodotto all’Ateneo un rilevante aggravio di costi, sia per quanto riguarda la manutenzione hardware/software delle piattaforme, sia per le risorse umane impiegate, spese che potevano essere azzerate da anni. In accordo con i responsabili dei Settori Help Desk di Chieti e del Settore Reti, Sistemi e Progettazione Web, nonché referenti di alcune delle piattaforme VM attive nel Data Center di Ateneo, è stata effettuata la disattivazione delle piattaforme che non sono più utili o fruibili. Ciò ha consentito una significativa riduzione del carico di lavoro del personale tecnico preposto alla gestione sistemistica e una importante riduzione del costo di manutenzione hardware/software delle piattaforme. Si evidenzia che sulla base dei costi indicati nel prospetto AGID Marketplace (<https://cloud.italia.it/marketplace/service/148>), il costo base annuo per l’erogazione del servizio cloud per una singola VM è pari a 3.750 euro (prezzo base: 3.250 euro + costo di attivazione: 500 euro). Sulla base di quanto esposto, la riduzione del costo di almeno n. 11 VM ha consentito l’immediato risparmio per l’Ateneo di 41.250 euro.

- b) *Predisposizione di un piano di migrazione delle piattaforme VM presso il Data Center del CINECA.* La scelta del Cineca quale fornitore di servizi cloud è riconducibile alla delibera del Consiglio Direttivo dell’ANAC, n. 399 datato 8 maggio 2020 (Elenco delle amministrazioni aggiudicatrici e degli enti aggiudicatori che operano mediante affidamenti diretti nei confronti di proprie società in house), che, in attuazione di quanto previsto dall’art.3, comma 9, del decreto legge n. 1/2020, dispone l’iscrizione del Ministero dell’Università e della Ricerca e del Ministero dell’Istruzione nell’elenco, di cui all’articolo 192, comma 1, del d.lgs. 50/2016, degli enti che detengono il controllo analogo congiunto in relazione agli affidamenti in regime di “*in house providing*” al CINECA. Il piano di affidamento delle piattaforme VM nel Virtual Data Center dal CINECA, è basato su un documento tecnico condiviso con i tecnici del Consorzio per consentire una migliore qualificazione dei servizi e delle infrastrutture tecnologiche di Ateneo secondo specifici parametri di sicurezza e affidabilità, garantendo:
- il miglioramento dell’erogazione dei servizi offerti dalle VM in termini di accessibilità, usabilità e sicurezza;
  - l’interoperabilità dei servizi delle VM derivante dall’applicazione del modello Cloud della PA;
  - la riduzione del rischio di “*vendor lock-in*”, ovvero la creazione di un rapporto di dipendenza da un fornitore del servizio privato;
  - la resilienza, la scalabilità e la protezione dei dati contenuti nelle VM.
- c) *Analisi delle tempistiche e dei costi di migrazione e dei canoni annuo di locazione delle Virtual Machines.* È stato prodotto un documento tecnico che contiene un’analisi dettagliata dei tempi, costi e sulle tecniche di migrazione delle VM all’interno del Virtual Data Center del CINECA. In riferimento ai costi precedentemente evidenziati (punto elenco “a”) e riconducibili a quelli riportati nella pagina “Virtual Data Center - VDC AGID Marketplace”, va sottolineato che gli stessi sono stati oggetto di una scontistica, da parte del CINECA, riservata agli Atenei.

L'intera migrazione delle piattaforme è prevista per fine 2022.

**Azione dell'Ente: Attività di reingegnerizzazione del portale web di Ateneo e migrazione di tutti i portali dell'Università sul modello di "portale federato Cineca".** Sulla base dell'esigenza di attivare un processo di reingegnerizzazione del portale di Ateneo e dei relativi siti delle Scuole, dei Dipartimenti e dei Centri, come da indicazione pervenute dal Rettore, Prof. Sergio Caputi, è stato istituito un Gruppo di Lavoro avente per obiettivo la completa revisione dell'ecosistema Web di Ateneo e finalizzato ad un processo di analisi, progettazione e realizzazione di un nuovo layout grafico, una rinnovata user experience, una content strategy e una nuova architettura di fruizione delle informazioni da parte degli utenti. Le attività iniziali condotte dai componenti del Gruppo di Lavoro, sono state essenzialmente incentrate su analisi/verifiche/interviste condotte con alcuni referenti di Settori/Aree/Centri, nonché docenti dell'Ateneo. Conseguentemente, è stato possibile rilevare una serie di criticità evidenziate dai protagonisti delle interviste soprattutto per quanto concerne i diversi siti dipartimentali, in termini di fruibilità delle informazioni presenti (e mancanti), di accessibilità dei portali di Ateneo con riferimento alle specifiche indicate dall'AgID (Agenzia per l'Italia Digitale), sulle criticità in termini di fruibilità dei contenuti da dispositivi smartphone e tablet (interfacce responsive), e complessivamente sulla possibilità di realizzare un portale che possa garantire le seguenti caratteristiche:

- immediatezza;
- flessibilità e adattabilità;
- efficacia;
- modernità;
- semplicità e linearità;
- emozionalità;
- affidabilità, trasparenza, innovazione.

Il sito dovrà essere organizzato in maniera chiara, attraverso una strutturazione gerarchica dei contenuti, evitando duplicazioni e ridondanze, e dando risalto alle aree/contesti rappresentati nella home page di Ateneo. Grande attenzione dovrà essere riservata all'efficacia della comunicazione, all'usabilità e all'accessibilità dei portali web al fine di veicolare e rafforzare l'identità dei servizi offerti, a garantire il supporto agli utenti nella fruizione delle informazioni, ad accrescere la percezione del valore dei servizi offerti, a favorire la comunicazione destinata ai diversi targets. Le soluzioni creative dovranno essere improntate alla realizzazione di un portale il più possibile lineare, semplice e moderno, evitando proposte eccessivamente articolate dal punto di vista grafico e/o di complessa gestione. Dovrà essere altresì gestita e completata la transizione della piattaforma CMS Drupal alla versione 9. Dalle attività di analisi condotte, sono state individuate alcune funzionalità nevralgiche che rappresenteranno la base fondante su cui erigere il nuovo portale di Ateneo:

- Migrazione completa dei contenuti dal vecchio al nuovo portale e dai vecchi ai nuovi siti federati secondo le esigenze evidenziate dal Gruppo di Lavoro Web e dai referenti di Scuole, Dipartimenti e Centri che saranno identificati e successivamente indicati quali referenti delle diverse strutture;
- Realizzazione di un portale multilingue autonomo in lingua inglese, francese, cinese, spagnola, ucraina a supporto dell'internazionalizzazione, in versione ridotta, ovvero comprensivo delle attività riconducibili alla traduzione delle sole parti essenziali del sito (come attualmente avviene per la versione del portale in inglese *en.unich.it*);
- Realizzazione del Course Catalogue, ovvero del sistema di Offerta Formativa basato su piattaforma web e derivante dai dati autoritativi disponibili sui gestionali CINECA. Il Course Catalogue dovrà interfacciarsi con i database di U-GOV per l'estrazione dei dati e dovrà essere fruibile sia da dispositivi fissi che da dispositivi mobili, onde consentire la consultazione dell'offerta formativa in maniera agile e veloce anche in lingua inglese;

- Realizzazione di una Dashboard Docente che possa ad ogni docente di gestire in totale e completa autonomia tutti i dati riconducibili al proprio profilo (foto, curriculum, pubblicazioni, etc.). La Dashboard dovrà rappresentare l'elemento nevralgico di accesso rapido a tutti gli applicativi e le funzionalità degli stessi, sulla base dell'utilizzo di un'area di backoffice dedicate;
- Uniformare il layout dei siti dipartimentali di Ateneo (n.14), ivi incluse le "utilities" realizzate da alcuni Dipartimenti e meglio specificati in un apposito documento tecnico in fase di realizzazione da parte del Prof. Mobidoni;
- Realizzazione dei portali delle Scuole di Ateneo (n.4), basati su un unico modello standard condiviso e identificato sulla base delle esigenze manifestate dai Presidenti delle Scuole;
- Realizzazione dei portali dei Corsi di laurea (n.68), basati sul modello standard di sito di Dipartimento (dati autoritativi e redazionali);
- Realizzazione dei portali dei Centri e Settori di Ateneo (n.14), realizzati su un modello comune e condiviso secondo le esigenze dei referenti, in linea con quanto fatto per i dipartimenti;
- Realizzazione del nuovo portale dell'Orientamento e della Terza Missione (Placement), sulla base dell'adozione di un modello che dovrà essere di grande impatto emozionale, utilizzando le più moderne soluzioni comunicative e d'immagine, come, ad esempio, l'utilizzo di animazioni che rendano immediatamente fruibili i contenuti video che presentino anche le attività e le dotazioni del territorio. Il Portale dell'Orientamento dovrà essere sviluppato sulla base del modello adottato dall'Università "Ca Foscari" di Venezia, come da indicazioni tecniche ricevute dai Settori di riferimento;
- Realizzazione di una nuova piattaforma e-learning, maggiormente funzionale ed in grado di ottimizzare l'interazione studente-docente, evolvendo anche l'attuale piattaforma Moodle;
- Realizzazione del Portale delle Competenze, basato sull'utilizzo del portale UNIFIND dedicato alla disseminazione delle attività di Ateneo. Le competenze, le attività ed i risultati delle attività di ricerca censite attraverso i diversi moduli IRIS confluiscono nel portale UNIFIND, il quale deve consentire ai diversi stakeholder (pubblico, aziende, docenti e ricercatori, uffici ILO (Industrial Liason Office) e TTO (Technology Transfer Office) di navigare le competenze presenti in Ateneo. Il sistema deve essere aperto alla consultazione pubblica in rete, e deve consentire di favorire la collaborazione e lo scambio tra l'università ed il sistema economico produttivo;
- Realizzazione del Portale UdA/Territorio, finalizzato alla realizzazione di apposita sezione che possa consentire una interazione tra l'Ateneo e le aziende del territorio. La sezione specifica dovrà permettere all'Ateneo e alle aziende registrate sulla piattaforma di poter fruire di una dashboard in grado di gestire l'inserimento di una molteplicità di informazioni relative ad una serie di funzionalità (inserimento laureati in aziende, valutazione dei curricula studenti, offerte di lavoro e stages, etc). L'obiettivo è quello di realizzare un ecosistema digitale di scambio di informazioni per favorire l'incontro tra domanda e offerta in ambito lavorativo/professionale;
- Realizzazione del Portale Mobilità Docenti, finalizzato alla creazione di una sezione che consenta l'iscrizione ad un "elenco riservato" di docenti universitari interessati al trasferimento/scambio contestuale interateneo. All'interno del portale, che sarà ispirato all'articolo di legge: *Scambi/Trasferimenti reciproci tra docenti universitari*, Art. 7, comma 3, legge 240/2010 – (Norme in materia di mobilità dei professori e dei ricercatori), dovranno essere accessibili tutte le informazioni relative alla disponibilità dei docenti sul piano della mobilità tra università (inserimento e pubblicazione, su un apposito database disponibile on-line, bandi e offerte di lavoro nel settore della ricerca da parte di enti ed organismi, Curricula Vitae dei docenti, incrocio delle offerte di lavoro e delle richieste, attraverso un sistema automatico che prenda in considerazione i criteri comuni delle offerte e delle richieste, consultazione per le organizzazioni

registrate nel database dei CV dei ricercatori presenti all'interno di un ulteriore database, con possibilità di selezione e combinazione personalizzata dei criteri di ricerca).

La presentazione del nuovo portale di Ateneo è prevista per fine 2023.

**Punto OB.3.2 - Aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni - Linea d'azione CAP3.PA.LA07 – Oggetto: Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e PagoPA e dismettono le altre modalità di autenticazione e pagamento associate ai propri servizi online.**

**Periodo: 2020-2021**

**Azione dell'Ente: Conclusione attività di sperimentazione dell'utilizzo della firma digitale mediante l'applicazione U-SIGN integrata con il sistema di gestione documentale Titulus.** Con riferimento all'adozione dell'applicazione U-SIGN del Cineca per la gestione della firma digitale per tutte le strutture dell'Ateneo ed in funzione della conseguente integrazione con il sistema di gestione documentale Titulus, si evidenzia che sono state condotte e completate le attività di sperimentazione e test da parte del Gruppo di Lavoro sull'utilizzo della firma digitale in Ateneo. La data di attivazione della firma digitale in Ateneo è fissata per settembre 2021.

**Azioni dell'Ente: Studio di fattibilità per l'adesione al sistema Identity Management per l'accesso federato (IDEM).** IDEM è la Federazione italiana di Infrastrutture di Autenticazione e Autorizzazione della comunità dell'istruzione e della ricerca, gestita e coordinata dal GARR (Gruppo per l'Armonizzazione delle Reti della Ricerca), ed opera all'interno della comunità dell'istruzione e della ricerca connessa alla rete GARR, supportando l'adozione di un framework comune per l'accesso alle risorse on line. Possono entrare a far parte della Federazione IDEM, in qualità di membri, tutti gli enti connessi alla Rete Italiana dell'Università e della Ricerca. Possono inoltre aderire alla Federazione IDEM, in qualità di partner, organizzazioni terze (ad esempio editori, fornitori di software o servizi online, ecc), purché forniscano contenuti o servizi che siano ritenuti utili alla Comunità GARR. IDEM basa i suoi servizi sullo standard SAML (Security Assertion Markup Language), tecnologia che permette lo scambio di dati di autenticazione e autorizzazione (asserzioni) tra domini di sicurezza distinti denominati *identity provider* (entità che fornisce informazioni di identità) e *service provider* (entità che fornisce servizi). Il formato delle asserzioni SAML è basato su XML. L'uso dello standard SAML è finalizzato alla risoluzione del problema del Web Single sign-on (SSO), una tecnica che consente ad un utente di effettuare un'unica autenticazione valida per diversi sistemi software o risorse informatiche per le quali è abilitato. Grazie al servizio di federazione gli Identity Provider possono fornire ai propri utenti meccanismi di SSO e protezione della privacy e i Service Provider possono ottenere un miglior controllo degli accessi verso le risorse protette eliminando la gestione account utenti che viene demandata ai sistemi di gestione delle identità degli Identity Provider. Tramite IDEM i membri che hanno aderito al servizio (che attualmente ammontano a n.111) possono garantire l'erogazione ai propri utenti di numerosi servizi e risorse, come biblioteche digitali, riviste, pubblicazioni scientifiche, reti Wi-Fi, piattaforme di e-learning, registro elettronico. Ad esempio, se un utente si collega ad una risorsa web offerta da un fornitore di servizi di terze parti, come potrebbe essere un servizio di consultazione di una rivista elettronica, scegliendo la modalità di login "Accesso istituzionale" egli viene rediretto alla pagina della propria Istituzione di appartenenza utilizzando le medesime credenziali istituzionali usate per l'accesso ai servizi interni. Se correttamente autenticato, il sistema di identità istituzionale trasmette al fornitore di servizi l'identità dell'utente, rappresentata da un insieme minimo di attributi. Il fornitore di servizi utilizza quindi queste informazioni per autorizzare l'utente all'accesso alla risorsa web. Pertanto, sulla base dell'esigenza di incrementare la sicurezza degli accessi degli utenti dell'Ateneo (studenti e personale), e per consentire l'utilizzo di un sistema di autenticazione nazionale per l'accesso alle banche dati delle strutture federate e a quelle offerte dal nostro Ateneo, si ritiene improcrastinabile l'adesione

a IDEM. Si evidenzia altresì che nell'anno in corso sono pervenute diverse richieste di adesione a IDEM da parte di alcuni Settori dell'Ateneo. In funzione di quanto esposto, è stata attivata, nel periodo di riferimento, una interazione tecnica con il CINECA, la cui struttura ha la responsabilità della gestione tecnica di IDEM, per verificare le procedure e le tempistiche di attivazione del servizio le quali sono state completate nel 2021.

**Linea d'azione CAP3.PA.LA13 - Le PA e i gestori di pubblici servizi interessati adottano lo SPID e la CIE by default: le nuove applicazioni devono nascere SPID e CIE-only a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID o CIE.**

**Periodo: 2020-2021**

**Azioni dell'Ente: Studio di fattibilità per l'adesione al Sistema Pubblico di Identità Digitale (SPID).** SPID è il sistema unico di accesso con identità digitale ai servizi online della pubblica amministrazione italiana e dei privati che intendono aderire al servizio. Istituito nel 2014, previsto dal Codice dell'Amministrazione digitale (art. 64) e attivo dal 2016, è gestito dall'Agenzia per l'Italia Digitale (AGID) con il coordinamento del Dipartimento per la Trasformazione digitale. SPID ha l'obiettivo di essere il punto di accesso semplice, sicuro e protetto a tutti i servizi pubblici online e dei privati aderenti da qualsiasi dispositivo: computer, tablet e smartphone. Pertanto, sia i cittadini che le imprese possono accedere a tali servizi con un'identità digitale unica che ne permette l'accesso e la fruizione da qualsiasi dispositivo. È stato introdotto grazie al moltiplicarsi di servizi online che costringe i cittadini ad avere un numero sempre crescente di credenziali di accesso. Consente, per mezzo di un unico set di credenziali, di accedere a qualsiasi servizio web. L'identità SPID può essere ottenuta dai cittadini maggiorenni, in possesso di un documento di identità italiano in corso di validità (carta d'identità, patente, passaporto). È composta da una coppia di credenziali (username e password) strettamente personali (livello di sicurezza 1) a cui può essere associata, in fase di accesso ai servizi, un'ulteriore verifica di sicurezza (la generazione di un codice temporaneo di accesso OTP o l'utilizzo di un'app per i livelli di sicurezza 2 o 3). L'identità SPID è anche la chiave di accesso ai servizi pubblici europei. Da settembre 2019 i cittadini italiani possono accedere con SPID ai servizi online di 23 Stati membri aderenti al nodo italiano "Login with eIDAS", resi disponibili grazie all'interoperabilità europea delle identità digitali, a cui l'Italia è stata la seconda nazione, dopo la Germania, ad aderire. Secondo il Decreto Semplificazioni (decreto legge n. 76/2020), entro il 28 febbraio 2021 tutte le amministrazioni locali e centrali, gli enti pubblici e le agenzie, dovranno integrare SPID e la Carta d'Identità Elettronica (CIE), per l'accesso ai servizi da parte dei cittadini, come sistemi di autenticazione rilasciati, uniformando l'accesso ai servizi pubblici digitali in tutto il Paese. Le vecchie credenziali potranno essere valide fino a naturale scadenza e non oltre il 30 settembre 2021. L'identità SPID è rilasciata dai Gestori di Identità Digitale (Identity Provider), soggetti privati accreditati da AGID che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti. È possibile richiedere l'identità SPID al gestore che si preferisce e che più si adatta alle proprie esigenze. L'identità SPID si ottiene facendone richiesta a uno degli identity provider (gestori di identità digitale), che è possibile scegliere liberamente tra quelli autorizzati dall'Agenzia per l'Italia digitale. Il gestore, dopo aver verificato i dati dell'utente, emette l'identità digitale, rilasciando le credenziali. L'identità SPID è costituita da credenziali con caratteristiche differenti in base al livello di sicurezza richiesto per l'accesso. Sul piano della sicurezza, come già evidenziato, esistono tre diversi livelli di accesso:

- ☒ il primo livello permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente;
- il secondo livello permette l'accesso con nome utente e password più un codice temporaneo di accesso (one-time password), fornito tramite SMS o app;
- ☒ il terzo livello, oltre al nome utente e la password, richiede un supporto fisico per l'identificazione, ad esempio una smart card.

SPID supporta l'autenticazione unica Single Sign-On (SSO), pertanto, dopo aver fatto l'accesso per un servizio, non è necessario ripetere l'autenticazione se si accede ad altri servizi, ma è una funzione attiva solo per il primo livello. Dal mese di novembre 2019 tutti i gestori di Identità Digitale si sono impegnati a fornire per sempre le credenziali SPID di livello 1 e 2 ai cittadini italiani gratuitamente.

Sulla base di quanto evidenziato, anche l'Università "G. D'Annunzio" di Chieti-Pescara è chiamata ad adeguare la propria infrastruttura tecnologica per consentire ai propri utenti di accedere ai servizi erogati dall'Ateneo. A tal proposito, si sottolinea che a luglio del 2016, il Cineca, in collaborazione con l'università di Torino, ha sviluppato un Gateway che consente agli Atenei di aderire a SPID (Figura 1). Sulla base dell'offerta del servizio, le università che hanno aderito sono:

- Università luav di Venezia;
- ☒ IUSS Scuola Universitaria di Pavia;
- Università degli Studi di Bari;
- Università degli Studi di Bergamo;
- Università degli Studi di Brescia;
- Università degli Studi della Calabria;
- Università degli Studi di Ferrara;
- Università degli Studi di Firenze;
- Università degli Studi di Macerata;
- Università degli Studi di Messina;
- Università degli Studi di Milano-Bicocca;
- Università degli Studi del Molise;
- Università degli Studi di Modena e Reggio Emilia;
- Università degli Studi della Campania "Luigi Vanvitelli";
- Università degli Studi dell'Insubria;
- Università degli Studi di Padova;
- Università degli Studi di Perugia;
- Università degli Studi di Pisa;
- Università degli Studi di Pavia;
- Università degli Studi del Salento;
- Università degli Studi di Teramo;
- Università per Stranieri di Siena;
- Università degli Studi di Trento;
- Università degli Studi di Torino;
- Università degli Studi di Trieste;
- Università degli Studi di Udine;
- Università degli Studi dell'Aquila;
- Università degli Studi Cà Foscari di Venezia;
- Università Politecnica delle Marche;
- Università degli Studi di Verona.

Si evidenzia altresì che in data 29.09.2015, con delibera n.451 (UOR: Settore Infrastrutture IT e TLC, prot.n. 0042355 del 29.09.2015), il Consiglio di Amministrazione dell'Ateneo ha approvato l'affidamento al Cineca della gestione dei servizi delle identità digitali di Ateneo basato su directoy di server Lightweight Directory Access Protocol - LDAP (riferimento relazione tecnica denominata "*Servizi di Identity management, Single sign-on e federazione per l'Ateneo*"). Sulla base dell'esistenza di questo affidamento, a dicembre 2020 il sottoscritto ha contattato il Cineca per verificare le tempistiche e le attività da condurre per l'attivazione di SPID in Ateneo. Una prima analisi è stata condotta sulla tecnologia di autenticazione utilizzata per l'accesso ai sistemi informatici dell'università, basata sulla versione 3.3.4. dell'Identity Provider (IdP) Shibboleth, la quale rende disponibile anche la funzione di Single Sign-On (SSO), ovvero la possibilità per l'utente di accedere a tutti i servizi a cui è abilitato. Entrambi i server (IdP e SSO) sono in hosting presso il Datacenter del Cineca.

L'IdP è stato esteso per consentire:

- l'autenticazione con credenziali rilasciate dal Sistema pubblico di identità digitale (SPID) e la riconciliazione di tali identità con le identità locali all'organizzazione di appartenenza dell'utente;
- l'autenticazione multifattore (MFA);
- il collegamento in SSO di applicazioni che utilizzano il protocollo OAuth (es.: app mobile);
- la compatibilità con le regole definite dall'organizzazione a cui appartiene l'utente per il ciclo di vita delle password (es.: modifica forzata della password perché scaduta, blocco dell'utente in caso di tentativo fraudolento di utilizzo delle credenziali, gestione history delle password utilizzate)

Tale estensione consente:

- di far convivere l'autenticazione dell'organizzazione con quella SPID;
- di realizzare politiche di riconciliazione più o meno complesse, in base alle esigenze dell'organizzazione;
- di concentrare in un unico punto gli obblighi normativi previsti per chi utilizza gli SPID in termini di monitoraggio, compliance e governance;
- di accreditare un solo servizio dell'organizzazione su SPID (il gateway) e guadagnare autonomia nell'aggiunta di nuovi servizi locali con autenticazione su SPID
- di aggregare in un solo punto gli attributi rilasciati dalle Attribute Authority SPID, dagli IdP SPID e dalle fonti interne all'organizzazione per distribuirli ai Service Provider.

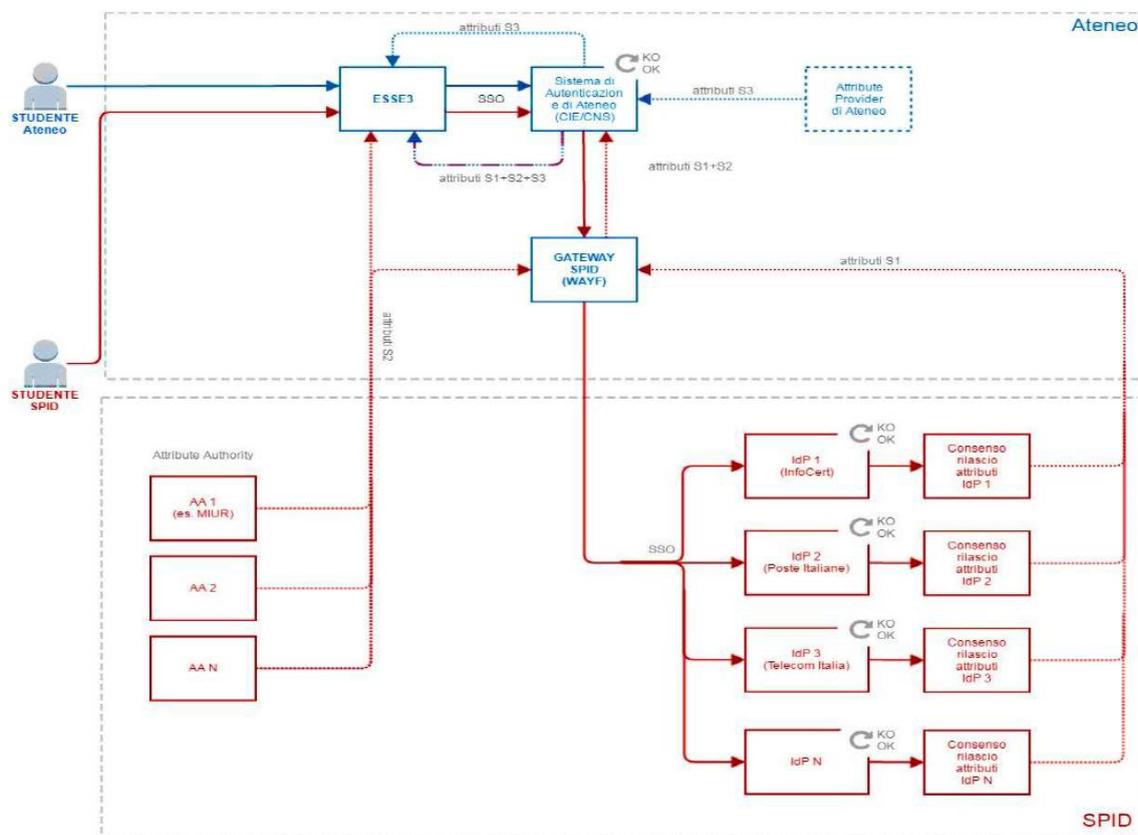


Figura 1 – Architettura del funzionamento di SPID in Ateneo

In rosso sono evidenziati i flussi di autenticazione di un utente con identità SPID. In blu sono evidenziati i flussi di autenticazione di un utente con identità fornita dall'Ateneo). Successivamente, è stata condotta un'attività tecnica per verificare la progressione delle azioni per l'attivazione di SPID. Le azioni da condurre in collaborazione con il Cineca sono:

- a. attivazione del Gateway SPID;

- b. riconfigurazione dell'applicazione ESSE3 per SSO/global logout;
- c. configurazione Shibboleth Idp in hosting per federazione GARR IDEM e eduGAIN.

Tali attività sono state condotte in un intervallo temporale, definito sempre dal Cineca, riconducibile ad una lista di prenotazioni che colloca l'Università di Chieti-Pescara nello "Slot" di Aprile 2021. Le procedure tecnico-amministrative da espletare con AGID e Cineca, saranno gestite anch'esse, parallelamente, nel periodo indicato. Le attività tecniche sono stimate in circa 30 giorni di lavoro. L'attivazione di SPID è stata condotta con successo nel corso del secondo semestre 2021.

**Azione dell'Ente: Attivazione del Sistema Pubblico di Identità Digitale (SPID) in Ateneo.** Sulla base dello studio di fattibilità condotto nel bimestre precedente sono state effettuate numerose attività tecniche relative all'implementazione di SPID in Ateneo, onde consentire l'accesso ai servizi erogati dall'Università di Chieti-Pescara al proprio personale e agli studenti. Le piattaforme attualmente fruibili con il sistema di autenticazione SPID sono:

- a) ESSE3 - Servizi Uda Online
- b) E-Learning - Piattaforma Moodle per la Teledidattica
- c) CORE - Servizi accessori per Personale e Studenti
- d) Titulus - Servizio di Protocollo Elettronico
- e) U-GOV - Sistema per la Governance degli Atenei
- f) Sprint - Performance Management
- g) U-Buy - Bandi di Gara e Avvisi Pubblici
- h) IRIS - Sistema Gestione Dati della Ricerca
- i) Portale UNICHQA - Area Riservata del Presidio di Qualità
- j) HR-Suite - Gestione Risorse Umane
- k) Pentaho - Business Intelligence
- l) U-Budget - University Budget Application
- m) Allocazione Costi - Pianificazione e Controllo
- n) Servizi Self-Service - Gestione Password e Account di Autenticazione

Nel periodo di riferimento, in particolare, sono state condotte le attività relative alla configurazione del sistema di Single Sign-On (SSO) e alla sua corretta funzionalità, ivi compresi i test di accesso tramite credenziali SPID ai diversi sistemi informatici dell'Ateneo che erogano servizi al personale e agli studenti. Utilizzando le credenziali SPID di alcuni utenti (del personale e degli studenti) che hanno collaborato ai test di funzionalità, è stato possibile identificare rapidamente le anomalie e gli errori relativi alle procedure di autenticazione. Di conseguenza, gli stessi sono stati rapidamente risolti anche grazie alla collaborazione del Cineca che gestisce il Gateway che consente a tutte le università che hanno aderito a SPID di poter gestire i processi di autenticazione degli utenti. Si evidenzia che il precedente sistema di autenticazione, basato sulla matricola del personale e degli studenti, rimarrà comunque attivo e fruibile in alternativa a SPID (figura 1).



Figura 1 – Maschera di accesso per l'autenticazione degli utenti ai servizi dell'Ateneo

**Azione dell'Ente: Analisi tecnica per adozione nuova U-APP Studenti.** Nell'ambito del progetto APP Studenti, il Cineca ha messo da tempo a disposizione delle università un'applicazione "mobile" customizzabile e fruibile per i diversi sistemi operativi presenti nei *device* disponibili sul mercato (iOS/Android). I servizi offerti dalla APP sono rivolti agli studenti, docenti, staff, futuri studenti o visitatori interessati alle attività dell'Ateneo. Tramite la APP gli studenti possono accedere in modo semplice e intuitivo ai principali servizi per la gestione della propria carriera universitaria. Fruibile anche come mezzo per avvicinare i futuri studenti all'Ateneo, consente di veicolare informazioni su eventi e iniziative, avvisi e comunicazioni a tutta la comunità universitaria. L'APP è suddivisa in *moduli* e progettata con un alto grado di flessibilità nella presentazione e nel layout: a seconda delle esigenze dell'Ateneo è possibile definire quali moduli attivare, la personalizzazione dell'ordine delle voci di menù, di parte della veste grafica e delle etichette di alcune sezioni dell'applicativo. Alcuni moduli sono ad accesso libero e presentano contenuti di interesse generale mentre altri sono raggiungibili dopo aver effettuato la login per ricevere contenuti personalizzati relativi alla propria situazione di studente. Sulla base di quanto esposto, è stata adottata una nuova versione di U-APP completamente rinnovata dal punto di vista della grafica e munita di alcune particolari funzionalità aggiuntive, come la funzione di accesso tramite SPID.

**Azione dell'Ente: Studio e analisi tecnica per configurazione accessi SPID "istituzionali" per il personale dell'Amministrazione centrale.** In funzione della necessità di consentire al personale di alcune Aree/Settori dell'Amministrazione centrale di accedere ai portali della PA (es. Inail, Inps, Ministero del lavoro, etc.), onde consentire l'espletamento delle quotidiane attività lavorative, è stata condotta un'indagine inerente i diversi gestori, operanti nel mercato nazionale, in grado di offrire servizi di accesso SPID di tipo "professionale". Tale urgenza è stata dettata dalla necessità di poter consentire al personale delle strutture di accedere alle piattaforme della PA per mezzo di credenziali di tipo "istituzionale". È stata condotta una ricognizione interna all'Ateneo che ha consentito la corretta individuazione degli utenti che necessitavano di questa tipologia di accesso. Successivamente, sono state attivate le procedure per l'identificazione del Gestore di Identità Digitale (Identity Provider) in grado di fornire le specifiche credenziali SPID. Sulla base dell'indagine condotta dal Responsabile del Settore Patrimonio Immobiliare, Procedure per Bandi e Acquisti sotto soglia Pubblici Appalti – MEPA, è stato identificato il gestore *Register.it*, azienda italiana che opera nel settore della fornitura di servizi di registrazione di domini, hosting, protezione del brand e pubblicità in Rete, quale fornitore per le credenziali SPID per gli operatori dell'Amministrazione. Compilate le procedure di acquisto, sono state condotte le attività di installazione e configurazione dei profili-utente richiesti.

**Azione dell'Ente: Analisi e attivazione del sistema di autenticazione della Carta di Identità Elettronica (CIE) in Ateneo.** La Carta di Identità Elettronica (CIE) è uno strumento di identità digitale riconosciuto anche in

Europa, e con essa è possibile accedere in sicurezza ai servizi online della Pubblica Amministrazione italiana e di tutte le aziende private che decidono di utilizzare quale strumento di autenticazione e accesso ai propri servizi. Tutte le pubbliche amministrazioni devono rendere i propri servizi online accessibili tramite CIE per favorire e semplificare l'utilizzo dei servizi digitali da parte di tutti i cittadini. In conformità al Regolamento eIDAS (electronic Identification Authentication and Signature), Regolamento UE n. 910/2014, la CIE è stata infatti notificata alla Commissione Europea e agli altri stati membri con la pubblicazione nella Gazzetta Ufficiale dell'Unione europea C309 del 13 settembre 2019, ed è stata integrata con i relativi nodi eIDAS. Il nodo eIDAS italiano consente l'interoperabilità transfrontaliera dei sistemi di identità digitali (eID) e la circolarità delle eID negli stati membri dell'Unione Europea, per aumentarne l'efficienza nelle transazioni digitali transfrontaliere. Nell'ambito delle eID, il regolamento eIDAS ed il nodo italiano eIDAS consentono che la identità digitale di uno Stato membro possa essere utilizzata per accedere ai servizi online della pubblica amministrazione o di privati negli altri stati membri della Unione Europea. Di seguito viene illustrato il modello di funzionamento del nodo eIDAS tramite una infografica del Connecting Europe Facility (CEF) che illustra il caso in cui un cittadino europeo richieda di fruire del servizio online di un altro stato membro della UE.



### Fasi del Login eIDAS

1. Un cittadino tedesco vuole registrare online il suo nuovo indirizzo in Italia per accedere ad un servizio.
2. Per verificare l'identità del cittadino tedesco la pubblica amministrazione comunica con il nodo eIDAS nazionale.
3. Il nodo eIDAS nazionale trasmette la richiesta al nodo eIDAS in Germania.
4. L'identità del cittadino tedesco viene verificata dagli identity e attribute providers tedeschi.
5. L'identità del cittadino tedesco, dopo la corretta verifica, viene inviata alla pubblica amministrazione italiana che consente al medesimo di accedere al servizio online richiesto.

Nel dicembre 2019 il Ministero dell'Interno si è collegato al nodo eIDAS nazionale, ovvero un sistema che consente ad ogni utente italiano di poter accedere ai servizi online di altri Stati membri della UE (e viceversa di un cittadino straniero che chiede di accedere a fornitori di servizi italiani, pubblici o privati). Il regolamento eIDAS ha anche l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e per i mezzi di identificazione elettronica degli Stati membri, onde consentire di gestire in sicurezza tutte le interazioni elettroniche fra cittadini, imprese e pubbliche amministrazioni, innalzando

l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'UE. La possibilità offerta ai cittadini italiani di accedere ai servizi pubblici online degli Stati europei anche con CIE, oltre che con SPID, è già in vigore nei Paesi di seguito elencati e connessi al nodo eIDAS italiano: Lussemburgo, Danimarca, Estonia, Grecia, Lituania, Lettonia, Malta, Olanda, Norvegia, Slovacchia, Slovenia, Spagna, Regno Unito. In sintesi, il regolamento:

- fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;
- stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;
- istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Il regolamento eIDAS è stato emanato il 23 luglio 2014 e ha piena efficacia dal 1 luglio del 2016. In data 24 maggio 2021 è pervenuta in Ateneo una mail inoltrata dal Ministero degli Interni in cui si comunicava la possibilità di avviare la procedura di adesione al progetto *"Entra con CIE"* per permettere a tutti gli studenti dell'Ateneo di accedere, tramite CIE, a tutti i servizi online dell'università. Va evidenziato che ad oggi le carte di identità elettroniche rilasciate in Italia ammontano ad oltre 20 milioni. In funzione dell'adesione del Rettore, Prof. Sergio Caputi, al progetto *"Entra con CIE"*, formalizzato in data 25.06.2021 del *"Modulo per l'adesione delle pubbliche amministrazioni e dei soggetti privati allo schema di identificazione Entra Con CIE"*, sono state condotte le operazioni tecnico-amministrative iniziali finalizzate all'integrazione del sistema di autenticazione CIE con quello utilizzato in Ateneo e gestito dal Consorzio Cineca di Bologna. Sulla base di quanto esposto sono state espletate le seguenti attività:

- definizione degli "step" tecnici, in collaborazione con il personale del Cineca, per l'integrazione del sistema di autenticazione CIE con quello di Ateneo;
- configurazione del Gateway SPID per l'autenticazione con CIE;
- interazione con il Ministero degli Interni ed il Poligrafico dello Stato per il rilascio di n.2 CIE card di prova per la conduzione dei test necessari per la verifica del corretto funzionamento del sistema di autenticazione;
- configurazione del sistema di autenticazione CIE per l'accesso al servizio *"Esse3 - Sistema per la gestione degli studenti"*.

Va evidenziato che l'Università "G. d'Annunzio" di Chieti-Pescara, grazie alla rapidità di attivazione di questa nuova funzionalità, **è stata la terza università, a livello nazionale, che ha attivato il sistema di autenticazione CIE, dopo l'Università degli Studi di Milano e l'Università degli Studi di Ferrara.**

***Azione dell'Ente: Attivazione del sistema di autenticazione della Carta di Identità Elettronica (CIE) in Ateneo.***

In data 12.01.2022, in conformità al Regolamento eIDAS (Regolamento UE n.910/2014), sulla base delle attività condotte nel periodo di riferimento della presente relazione, è stato attivato il servizio di autenticazione con Carta di Identità Elettronica (CIE) per il personale T/A TAB, docente e studenti. Di conseguenza, tutti i servizi relativi ai sistemi informativi del Cineca sono attualmente fruibili anche con CIE. L'Università "G. d'Annunzio" di Chieti-Pescara, tra le prime in Italia, compare ora tra gli Erogatori di servizi abilitati a CIE del Ministero degli Interni (Immagine 1). Le diverse modalità di autenticazione offerte agli utenti per l'accesso ai servizi di Ateneo sono evidenziate in una nuova pagina web che racchiude le tre modalità di accesso (Immagine 2-3-4).

## Federazione erogatori servizi

[Home](#) [Lista SP](#) [App CIE](#) [FAQ](#) [Manuale Tecnico](#) [Manuale Operativo](#)[Home](#) / [ListaSP](#)

## Erogatori di servizi abilitati

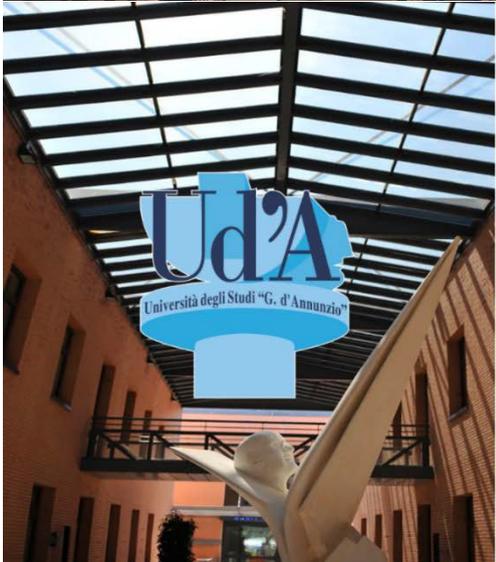
Pubbliche Amministrazioni

Soggetti privati

Le Pubbliche Amministrazioni che hanno integrato l'accesso con **ENTRA CON CIE** ai propri servizi sono le seguenti:

[Santo Stefano Ticino](#)[Sapienza Università di Roma](#)[UNIONE COMUNI MARMILLA](#)[UNIONE MONTANA DEL MONTE REGALE](#)[Unioncamere - Impresa in un Giorno](#)[Unioncamere - Registro delle Imprese](#)[Unione Campospinoso Albaredo](#)[Unione Dei Comuni Lombarda della Valletta](#)[Unione Dei Comuni Terre D'Acque](#)[Unione Dei Comuni Valle del Savio](#)[Unione Montana Valle Stura](#)[Unione Ovest Lago Varese](#)[Unione Riviera del Monferrato](#)[Unione Terre di Castelli](#)[Unione dei Comuni Lombarda Oltrepo' Centrale](#)[Unione di Comuni Collinari del Vergante Belgirate Lesa Meina](#)[Unione di Comuni Lombarda Mincio Po](#)[Unione di Comuni Lombarda Oltre Adda Lodigiano](#)[Universita' Degli Studi G. d'Annunzio di Chieti](#)[Universita' degli Studi di Firenze](#)

Immagine 1 - Erogatori di servizi abilitati a CIE del Ministero degli Interni



### Accedi a MyUd'A

Per accedere a questo servizio devi autenticarti  
Accedi a [sp-titulus-unich.cineca.it](https://sp-titulus-unich.cineca.it)

**ATENEO** SPID CIE

Nome utente

Password

**Accedi**

Futuri studenti, studenti, laureati, dottorandi e specializzandi  
• Rigenera la password  
• Serve aiuto?

Docenti e Personale T/A  
• Rigenera la password  
• Serve aiuto?

[Informativa sui cookie](#) | [Informativa sulla privacy](#)

### Accedi a MyUd'A

Per accedere a questo servizio devi autenticarti  
Accedi a [sp-titulus-unich.cineca.it](https://sp-titulus-unich.cineca.it)

**ATENEO** **SPID** CIE

SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedila ad uno dei gestori.

**Entra con SPID**

Maggiori informazioni  
Non hai SPID?  
Serve aiuto?

AgID Agenzia per l'Italia Digitale

### Accedi a MyUd'A

Per accedere a questo servizio devi autenticarti  
Accedi a [sp-titulus-unich.cineca.it](https://sp-titulus-unich.cineca.it)

**ATENEO** **SPID** **CIE**

**Entra con CIE**

CIE è lo schema di identificazione che consente l'accesso ai servizi digitali erogati in rete di pubbliche amministrazioni e privati, mediante l'impiego della CIE, come previsto dall'art. 64 del Codice dell'Amministrazione Digitale.

Maggiori informazioni sulla CIE

[Informativa sui cookie](#) | [Informativa sulla privacy](#)

Immagine 2-3-4 – Modalità di autenticazione utente basate su credenziali di Ateneo, SPID, CIE

**Azione dell'Ente: Adozione della firma digitale per tutte le strutture dell'Ateneo con integrazione al sistema di gestione documentale Titulus.** Con riferimento all'adozione della firma digitale per tutte le strutture dell'Ateneo con l'integrazione al sistema di gestione documentale Titulus, si evidenzia che la procedura di collegamento tra piattaforma U-SIGN e la piattaforma Titulus è stata completata nel periodo di riferimento.

**Azione dell'Ente: Analisi tecnica per l'attivazione dei servizi ERASMUS+ per gli studenti.** In data 13.08.2021, per mezzo email, è stato comunicato dal GARR l'attivazione, su base nazionale, del nuovo servizio ERASMUS+ per gli studenti italiani (<https://www.idem.garr.it/federazione-idem/blog/770-scatta-il-conto-alla-rovescia-per-l-accesso-ai-servizi-erasmus>). A partire dal primo settembre 2021, l'accesso ai servizi Erasmus+ per gli studenti italiani, ed in particolare all'Online Learning Agreement (<https://www.learning-agreement.eu>), è possibile solo per gli enti GARR che hanno un Identity Provider registrato nella Federazione IDEM ed esportato in eduGAIN, come nel caso dell'Ateneo di Chieti-Pescara. Per tutti gli enti che non fanno parte della rete GARR, quest'ultima, insieme ad INDIRE (Istituto nazionale di documentazione, innovazione e ricerca educative) che gestisce l'Agenzia nazionale Erasmus+, ha creato un Identity Provider ad hoc per permettere l'accesso anche ai loro studenti. Da settembre del 2021, pertanto, è obbligatorio rilasciare lo European Student Identifier (ESI), un sistema di identificazione digitale che consente agli studenti di essere correttamente identificati quando accedono ai servizi online di mobilità studentesca nei paesi dell'UE. Il sistema ESI, sviluppato dall'European Student Card Project, è progettato per facilitare la mobilità studentesca internazionale e la cooperazione transnazionale degli istituti di istruzione superiore. Si evidenzia che il team di MyAcademicID (<https://myacademic-id.eu/>) ha rivisitato il formato di ESI e ha pubblicato le nuove specifiche del formato con l'obiettivo di supportare al meglio i flussi online. Si sottolinea che MyAcademicID è un progetto finanziato dal programma Connecting Europe Facility nel 2019-2020, nel contesto dell'iniziativa European Student Card, nato per consentire agli studenti di autenticarsi per i loro studi all'estero utilizzando il proprio account studente di origine, grazie a eduGAIN, e per collegare le loro identità accademiche per mezzo dei nodi nazionali eIDAS e, di conseguenza, per abilitare il sistema European Student Identifier (<https://wiki.geant.org/display/SM/European+Student+Identifier>). Sulla base di quanto evidenziato, e per attivare velocemente il servizio ERASMUS+, è stata svolta un'attività in collaborazione con il CINECA, che gestisce l'Identity Provider IDEM con la collaborazione con i gestori della piattaforma MyAcademicID. Il servizio è stato reso disponibile a settembre 2021.

**Linea d'azione CAP1.PA.LA15 – Oggetto: Le PA devono pubblicare, entro il 23 giugno 2021, la dichiarazione di accessibilità per le APP mobili, tramite l'applicazione form.agid.gov.it**

**Periodo: 2021**

**Azione dell'Ente: Attivazione della nuova U-APP Studenti.** Nell'ambito del progetto di fruizione della nuova versione di U-APP per gli studenti dell'Ateneo, integrata con SPID sono state condotte tutte le attività tecniche di test di funzionalità e fruibilità della nuova versione della app, ora disponibile e fruibile gratuitamente in tutti gli "store" di applicazioni mobile.

**Linea d'azione CAP3.PA.LA20 - Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID connect, servizi per i minori e gestione degli attributi qualificati).**

**Periodo: 2021**

**Azione dell'Ente: Adozione della firma digitale per tutte le strutture dell'Ateneo con integrazione al sistema di gestione documentale Titulus.** Con riferimento al Codice dell'Amministrazione Digitale, Capo II, Documento informatico, firme elettroniche, servizi fiduciari e trasferimento di fondi, Decreto Legislativo

07.03.2005 n.82, G.U. 16.05.2005, ed in particolare all'Art.20 (Validità ed efficacia probatoria dei documenti informatici), 1-bis:

*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immutabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.*

Si evidenzia che l'Ateneo, onde consentire al personale docente di gestire online gli appelli degli esami di profitto autenticandosi via web nell'area riservata del portale di Ateneo, ha aderito dal 2015 al servizio di firma digitale offerto dal Cineca (ConFirma). Tale servizio consente l'integrazione di firma (remota e con smart card o token USB) negli applicativi Cineca. Conseguentemente, gli utenti titolari di firma digitale su smart card rilasciate da Certificatori Accreditati AgID, o di firma remota compatibile con l'attuale implementazione (Infocert, Aruba, TelecomItalia), hanno la possibilità di firmare digitalmente documenti nei formati previsti dalla normativa (PAdES, XAdES, CAdES), per le finalità istituzionali del loro ruolo.

In funzione delle indicazioni fornite da AgID in merito alla dematerializzazione delle attività amministrative e dal Codice dell'Amministrazione Digitale, sono state condotte delle attività finalizzate alla conduzione di un censimento delle strutture (Divisioni, Aree, Settori, Centri, etc.) che necessitavano del dispositivo di firma certa. L'adozione della firma digitale potrà consentire ai responsabili delle diverse strutture di poter utilizzare uno strumento basato sulla crittografia a chiave pubblica che possa garantire la sicurezza, l'accuratezza e l'autenticità dei documenti prodotti. Cionondimeno, tale innovazione consentirà a tutte le strutture dell'Amministrazione di raggiungere una completa digitalizzazione del processo di firma. Si evidenzia, che il sistema di gestione documentale del Cineca in uso in Ateneo (Titulus), consente la gestione del flusso automatico per la produzione di documenti digitali in partenza. Tale flusso prevede un iter di approvazione che inizia con l'inserimento di una bozza da parte di un operatore proponente, prosegue con la valutazione della bozza da parte di vari approvatori vari livelli gerarchici e termina con la sottoscrizione digitale (da parte di chi ne ha l'autorità) e la protocollazione automatica. Per l'attivazione del sistema di Firma Digitale Remota su Titulus il Cineca offre una specifica soluzione, meglio nota come U-SIGN, che consente:

- di personalizzare graficamente l'interfaccia utente sulla base dell'Identità di Ateneo;
- di profilare gli utenti che possono essere abilitati all'utilizzo del sistema;
- di analizzare le tipologie di documenti che possono essere firmati digitalmente dagli utenti accreditati;
- di creare degli ambienti di collaudo ed esercizio;
- di poter integrare le diverse applicazioni fruibili per il processo di firma digitale (Confirma, Gdrive, DropBox, ...).

Con l'adozione di U-SIGN è ora possibile automatizzare il processo di firma digitale nella fase di protocollazione dei documenti.

**Azione dell'Ente:** *Aggiornamento dei formati trattati dal sistema di conservazione di Ateneo sulla base delle nuove Linee Guida dell'AgID. In riferimento alla determinazione n. 371/2021 del 17 maggio 2021 - Modifiche testo Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, allegato 5 - Metadati, allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati ed estensione dei termini di entrata in vigore, è stata condotta un'attività di verifica sulla correttezza dei formati dei files oggetto delle operazioni di riversamento sulla piattaforma CONSERVA del Cineca. Tale attività è riferibile*

all'entrata in vigore delle Linee Guida AgID (Allegato 2 – *Formati di file e riversamento, individuano i formati idonei alla conservazione a lungo termine*) che stabiliscono l'adeguamento dei nuovi formati di files al 1 gennaio 2022. L'attività, svolta in collaborazione con il Cineca, previa verifica dei formati, ha consentito l'adozione del nuovo Manuale di Conservazione – Allegato 8 Formati accettati, di seguito riportato:

## MANUALE DI CONSERVAZIONE

### Allegato 8 – Formati accettati

Versione. 1.0 del 01/10/2021

CINECA

## Manuale di Conservazione

### Allegato 8 – Formati accettati

## Consorzio Interuniversitario CINECA

#### INFORMAZIONI SULLA CLASSIFICAZIONE DEL DOCUMENTO

LIVELLO DI CLASSIFICAZIONE		DATA DI CLASSIFICAZIONE O DI MODIFICA ALLA CLASSIFICAZIONE INIZIALE	RESPONSABILE DELLA CLASSIFICAZIONE DEL DOCUMENTO	DESTINATARI DEL DOCUMENTO
Riservato				
Ad uso interno				
Di dominio pubblico	X	01/10/2021	Massimiliano Valente	Titolari dell'oggetto di conservazione, Personale Cineca

#### STATO/STORIA DELLE REVISIONI

Versione	Data	Paragrafo rev.	Oggetto dalla revisione	Autore/i principale della revisione	Altri contributi	Validato
1.0	01/10/2021		Emissione	Mariagrazia Mingrone Nicola Carofiglio	Alessandro De Angelis	Massimiliano Valente

### **1. Introduzione**

Il presente allegato riporta l'elenco completo dei formati accettati dal Sistema di Conservazione Conserva.

I criteri di scelta dei formati seguiti per la stesura dell'elenco e necessari a garantire la leggibilità e la reperibilità del documento informatico sono i seguenti:

- apertura
- sicurezza
- portabilità
- funzionalità
- supporto allo sviluppo
- diffusione

La valutazione dei formati è stata condotta seguendo le disposizioni previste dall'Allegato 2 - Formati di file e riversamento delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

L'elenco include tutti i formati ritenuti idonei alla conservazione oppure estremamente diffusi all'interno degli Enti Titolari dell'oggetto di conservazione.

### **2. Modalità di aggiornamento**

L'elenco viene mantenuto aggiornato a seguito di valutazioni periodiche effettuate dal team del Servizio di Conservazione in relazione, ad esempio, a:

- evoluzioni tecnologiche
- disposizioni normative
- richieste specifiche dei Titolari dell'oggetto di conservazione

L'elenco viene reso pubblico e messo a disposizione di tutti i Titolari dell'oggetto della conservazione di [Cineca](https://wiki.u-gov.it/confluence/display/Conserva/Conserva+-+Il+servizio+di+conservazione+CINECA) (<https://wiki.u-gov.it/confluence/display/Conserva/Conserva+-+Il+servizio+di+conservazione+CINECA>)

### 3. Formati di file accettati

#### 3.1 Legenda

L'elenco è suddiviso in base alla tipologia di formato secondo quanto riportato dall'Allegato 2 - Formati di file e riversamento delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (ad esempio Archivi compressi, Caratteri tipografici, Documenti impaginati, etc).

Per ciascun formato viene indicato:

- **Nome:** nome completo del formato.
- **Estensione:** estensione del file.
- **Tipo Mime:** codifica MIME del formato. In particolare, un tipo Mime è composto da un identificatore del tipo seguito da un identificatore del sottotipo. Ad esempio application/pdf.
- **Restrizioni:** eventuali vincoli nell'uso del formato, necessari a incrementare il livello qualitativo della conservazione. Ad esempio l'uso del PDF/A.

#### 3.2 Elenco formati

Nome	Estensione	Tipo Mime	Restrizioni
<b>Archivi compressi – 2.13 Allegato 2 LLGG</b>			
GNU Zip	.gzip	application/gzip	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
Java Archive file format	.jar	application/jar-archive	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
Immagine di volume ISO9660	.iso	application/x-iso9660-image	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
UNIX Standard Tape Archive (TAR)	.tar	application/x-tar	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
7-Zip compressed archive format	.7z	application/x-7z-compressed	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.

# MANUALE DI CONSERVAZIONE

CINECA

## Allegato 8 – Formati accettati

Versione. 1.0 del 01/10/2021

Zip	.zip, .zipx	application/zip	All'interno dell'archivio compresso NON devono essere presenti: (1) archivi compressi e (2) formati NON previsti dal seguente allegato.
<b>Audio e Musica – 2.9 Allegato 2 LLGG</b>			
[Broadcast] Waveform File	.wav, .bwf, .rf64	audio/wave	Non deve presentare compressione.
<b>Caratteri tipografici – 2.8 Allegato 2 LLGG</b>			
OpenType®	.otf	application/x-font-otf	Valido solo come file allegato e non come file principale
OpenType®	.otf	font/otf	Valido solo come file allegato e non come file principale
TrueType®	.ttf	application/x-font-ttf	Valido solo come file allegato e non come file principale
TrueType®	.ttf	font/ttf	Valido solo come file allegato e non come file principale
Web Open Font Format	.woff2	font/woff2	Valido solo come file allegato e non come file principale
Web Open Font Format	.woff	application/font-woff	Valido solo come file allegato e non come file principale
<b>Contenitori e pacchetti di file multimediali – 2.12 Allegato 2 LLGG</b>			
MPEG-4, Part 14	.mp4, .m4a, .m4v	audio/mp4	
MPEG-4, Part 14	.mp4, .m4a, .m4v	video/mp4	
Digital Cinema Distribution Master	.tif/.tiff	image/tiff	Non deve presentare compressione.
<b>Dati strutturati – 2-3 Allegato 2 LLGG</b>			
JavaScript Object Notation	.json	application/json	
JavaScript Object Notation for Linked Data	.jsonld	application/ld+json	
Structured Query Language	.sql	application/sql	
Comma-Separated Value	.csv	text/csv	
<b>Documenti impaginati – 2.1 Allegato 2 LLGG</b>			
Portable Document Format	.pdf	application/pdf	Solo PDF/A
WordProcessingML OOXML Extension	.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Solo profilo Strict

# MANUALE DI CONSERVAZIONE

## Allegato 8 – Formati accettati

Versione. 1.0 del 01/10/2021

WordProcessingML OOXMLExtension	.dotx	application/vnd.openxmlformats-officedocument.wordprocessingml.template	Solo profilo Strict
Open Document Text	.odt	application/vnd.oasis.opendocument.text	
<b>Fogli di calcolo e presentazioni multimediali – 2.5 Allegato 2 LLGG</b>			
PresentationML OOXMLExtension	.pptx, .ppsx, .potx	application/vnd.openxmlformats-officedocument.presentationml.presentation	Solo profilo Strict
<b>Immagini raster - 2.6 Allegato 2 LLGG</b>			
JPEG File Interchange Format (JFIF)	.jpeg	image/jpeg	
JPEG File Interchange Format (JFIF)	.jpg	image/jpg	
Portable Network Graphics	.png	image/png	
<b>Immagini vettoriali e modellazione digitale – 2.7 Allegato 2 LLGG</b>			
Autodesk® AutoCAD® Drawing	.dwg, .dwt	application/acad	
Autodesk® AutoCAD® Drawing	.dwg, .dwt	image/vnd.dwg	
Scalable Vector Graphics	.svg	image/svg+xml	
Scalable Vector Graphics	.svgz	image/svg+xml+zip	
<b>Ipertesti – 2.2 Allegato 2 LLGG</b>			
Extensible Hypertext Markup Language	.xhtml, .html	application/xhtml+xml	Solo se presente foglio di stile (CSS)
Extensible Markup Language	.xml	application/xml text/xml	
Extensible Stylesheet Language Transformations	.xslt	application/xslt+xml	
Cascaded Style Sheet	.css	text/css	
Hypertext Markup Language	.html, .htm	text/html	

Extensible Stylesheet Language	.xsl	text/xsl	
<b>Posta elettronica - 2.4 Allegato 2 LLGG</b>			
Electronic Mail Format	.eml	application/email	
“Default” Mbox Database Format	.mbox	application/mbox	
<b>Altri formati individuati da Cineca non indicati nelle Linee Guida</b>			
Plain Text	.txt	text/plain	

Le attività condotte hanno consentito di verificare la correttezza dei formati dei files dati onde consentire la funzionalità delle operazioni di riversamento sulla piattaforma CONSERVA del Cineca.

**Azione dell’Ente: Attività di sperimentazione dell’utilizzo della firma digitale mediante l’applicazione U-SIGN integrata con il sistema di gestione documentale Titulus.** Con riferimento all’adozione dell’applicazione U-SIGN del Cineca per la gestione della firma digitale per tutte le strutture dell’Ateneo, ed in funzione della conseguente integrazione con il sistema di gestione documentale Titulus – attività condotta nel periodo di riferimento di questa relazione - si evidenzia che nel periodo è stato creato uno specifico “gruppo di lavoro” finalizzato alla conduzione di un periodo di sperimentazione pratica dell’utilizzo della firma digitale. Tale sperimentazione ha visto il coinvolgimento di alcuni referenti delle Aree/Settori dell’Ateneo, opportunamente selezionati sulla base della verifica della disponibilità individuale manifestata. La sperimentazione è stata incentrata sulla conduzione di una molteplicità di prove e simulazioni di registrazione di documenti firmati digitalmente, onde consentire:

1. la verifica dell’affidabilità della procedura e delle eventuali esigenze di personalizzazione dei flussi di workflow su Titulus;
2. la garanzia che le figure “autorizzative” coinvolte nelle operazioni di firma digitale siano esattamente quelle identificate per le diverse procedure amministrative.

Sulla base delle verifiche svolte, ed in funzione delle rispettive esigenze riscontrate dal gruppo, è stata evidenziata la necessità di strutturare un apposito “workflow” in grado di garantire il corretto funzionamento del flusso autorizzativo dei documenti da firmare digitalmente all’interno dell’Ateneo. Di conseguenza, è stato possibile disegnare un “flusso flessibile” basato sul funzionamento di seguito descritto:

1. L’utente registra la bozza del documento;
2. L’utente indica i nominativi degli “approvatori” (massimo 3);
3. L’utente indica i nominativi dei “firmatari” (massimo 3);
4. Gli “approvatori”, in ordine di scelta, approvano la bozza;
5. I “firmatari”, in ordine di scelta, firmano digitalmente il documento;
6. Dopo che l’ultimo firmatario ha firmato digitalmente il documento, quest’ultimo viene protocollato automaticamente dall’utente che ha creato la bozza.

L’utilizzo di un’unica applicazione per la firma digitale garantirà la riduzione della possibilità, da parte degli utenti, di commettere errori durante la fase di registrazione dei documenti.

### 3 AZIONI PROGRAMMATE NEL SECONDO SEMESTRE 2022 E NELL'ANNO 2023

#### 3.1 SERVIZI

Come riportato nel Piano Triennale per l'Informatica nella PA 2020–2022, assume particolare rilevanza il miglioramento della qualità dei servizi pubblici digitali onde consentire un crescent incremento del loro utilizzo da parte degli utenti. L'obiettivo è quello di fornire servizi completamente digitali e facilmente fruibili per soddisfare l'esperienza degli utenti così come evidenziato nell'art. 7 del Codice dell'Amministrazione Digitale (CAD) - Diritto a servizi on line semplici e integrati. L'Ateneo, pertanto, intende perseguire gli obiettivi di seguito evidenziati:

- Semplificazione delle procedure per progettare servizi digitali sicuri e fruibili.
- Rendere, ove possibile, ogni servizio accessibile, inclusivo e utilizzabile da qualsiasi dispositivo tecnologico.
- Accrescere le competenze informatiche del personale dell'Ateneo secondo il Syllabus delle "Competenze digitali per la PA", document che descrive l'insieme minimo delle conoscenze e abilità che ogni dipendente pubblico, non specialista IT, dovrebbe possedere per partecipare attivamente alla trasformazione digitale della pubblica amministrazione. Esso rappresenta lo strumento di riferimento sia per l'attività di autoverifica delle competenze digitali che per la definizione di corsi volti a indirizzare i fabbisogni formativi rilevati. L'obiettivo generale del Syllabus è fare in modo che tutti i dipendenti pubblici siano in grado di operare attivamente in modo sicuro, consapevole, collaborativo e orientato al risultato all'interno di una pubblica amministrazione sempre più digitale. Il Syllabus si concentra esclusivamente sugli aspetti pertinenti alle competenze digitali complementari richieste ad un dipendente pubblico che lavora in ambienti digitali.
- Implementare nuovi strumenti e metodologie di lavoro che possano garantire, sulla base del mantenimento delle modalità di erogazione del lavoro agile, l'innalzamento del livello di sicurezza sulla gestione dei dati e della sicurezza informatica.

Nel corso del 2023 le azioni dell'Ateneo saranno concentrate su alcuni ambiti quali:

- Miglioramento dell'esperienza d'uso e dell'accessibilità dei servizi.
- Progettazione e implementazione di percorsi formativi per il personale finalizzati all'incremento delle competenze digitali, come indicato nel Syllabus delle "Competenze digitali per la PA".
- Diffusione di linee guida operative per la creazione di pagine web e documenti non web accessibili, anche sulla base delle Linee guida sull'accessibilità degli strumenti informatici emanate da AgID.
- Monitoraggio dei servizi attraverso la piattaforma nazionale *open source* Web Analytics Italia, che fornisce statistiche in tempo reale utili a comprendere il comportamento degli utenti online, con l'obiettivo di ottenere un miglioramento continuo dell'esperienza utente;

I punti e le linee di azioni su cui saranno condotte specifiche attività nel corso del 2023 e riferibili al Piano Triennale per l'Informatica, sono di seguito riportate:

**Punto OB.7.2 (Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale).**

**Periodo: 2022-2023**

**Azioni dell'Ente: Progettazione e implementazione di percorsi formativi per il personale finalizzati all'incremento delle competenze digitali, come indicato nel Syllabus delle "Competenze digitali per la PA".**

**Periodo: 2021-2024**

**Azioni dell'Ente:** La connettività Internet attualmente è servita dalla "Convenzione Per i Servizi di Connettività tramite rete GARR", stipulato in data 15/06/2021 con durata di sei anni (2021 – 2027), così strutturato:

1. Fibra ottica spenta (dark fiber) per collegamento tra sede Viale Pindaro, 42 (PE) e sede Via dei Vestini, 31 (CH) con capacità di 20 Gbps (terminazione 2 x 10 Gbps) -VPN ottica;
2. Connettività tra Sede Pescara (PoP GARR c/o Telecom) e sede di Bologna (PoP GARR c/o INFN – CNAF) con capacità di 10 Gbps (terminazione 10G);
3. Connettività di Backup tra Sede Chieti (PoP GARR c/o Telecom) e sede di Roma (PoP GARR c/o CINECA) con capacità di 1 Gbps (terminazione 1G).

Per quanto concerne alcune sedi remote è stato attivato in data 06.04.2018 il contratto esecutivo OPA – "Servizi di Connettività nell'ambito del sistema pubblico di connettività 2 (SPC2)" che garantisce il collegamento di tali sedi tramite l'utilizzo di VPN protette ognuna da singolo firewall fisico.

**Linea d'azione CAP6.PA.LA05 - Le PA possono definire, in funzione delle proprie necessità, all'interno dei piani di formazione del personale, interventi sulle tematiche di Cyber Security Awareness.**

**Periodo: 2023-2025**

**Azioni dell'Ente:** *L'Ateneo si pronone di definire momenti di formazione e campagne informative finalizzate alla diffusione della cultura della sicurezza informatica tra il personale dell'Università.* Saranno adottati strumenti specifici che possano consentire, ad esempio, la simulazione e il monitoraggio di campagne di phishing, una tecnica efficace per incrementare il livello di consapevolezza sui rischi cyber legati al phishing. L'Agenzia per l'Italia Digitale ha promosso uno specifico progetto che si pone l'obiettivo di supportare tutte le Pubbliche Amministrazioni per l'adozione di una metodologia di Cyber Risk Management<sup>2</sup> sviluppata nell'ambito del Piano Triennale per l'informatica nella Pubblica Amministrazione. A tal proposito, l'AgID ha realizzato un tool di valutazione e trattamento del rischio cyber che consente ad ogni PA di effettuare le operazioni di self-assessment, i piani di trattamento e il monitoraggio delle iniziative volte a ridurre il livello di rischio informatico. L'Ateneo intende quindi adottare tale strumento per incrementare al fine di effettuare un self-assessment di sicurezza informatica, migliorare la consapevolezza sulle materie di cybersecurity e valutare le vulnerabilità e il livello di esposizione al rischio cyber

### **3.2 DATI E INTEROPERABILITA'**

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la pubblica amministrazione, di conseguenza è indispensabile garantire una maggiore efficacia all'attività amministrativa in tutti i processi che coinvolgono l'utilizzo dei dati, sia in riferimento alla condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali (art. 50 del CAD), sia per il riutilizzo dei dati, per altre finalità, secondo il paradigma degli *open data*. I dati pubblici costituiscono una risorsa per il Paese, di conseguenza risulta fondamentale condividere i propri dati con la PA, riconducibile al concetto di interoperabilità definito come la "caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi" (Art.1 c.1 l. ad del CAD). Un aspetto sul quale l'Ateneo intende compiere un ulteriore sforzo riguarda proprio l'ambito della

<sup>2</sup> <https://www.sicurezza.gov.it/cyber/>

gestione e protezione dei dati che ha subito un profondo mutamento fin dall'entrata in vigore del Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR) e dalla sua attuazione avvenuta a partire dal 25 maggio 2018. In questo ambito è necessario sensibilizzare l'utenza e il dipendente sulla corretta gestione e divulgazione del dato e sulla distinzione tra privacy, accesso generalizzato e trasparenza; tre paradigmi alla base di una corretta gestione dei dati e delle informazioni di proprietà dell'Ateneo.

### 3.3 PIATTAFORME

Le Piattaforme tecnologiche sono soluzioni che offrono molteplici funzionalità che assumono caratteri di trasversalità e riusabilità nella digitalizzazione dei processi e dei servizi della PA. L'impiego di tali piattaforme permette un sostanziale riduzione del carico di lavoro delle Pubbliche Amministrazioni, riducendo tempi e dei costi di erogazione dei servizi e innalzando il livello della sicurezza, integrità e disponibilità dei dati. Le Piattaforme, in una visione funzionale, possono essere suddivisi nelle seguenti categorie:

- *Process service*. Piattaforme che realizzano digitalmente un processo completo (ad esempio l'approvvigionamento realizzato tramite gli strumenti di *Public e-procurement*) di cui le PA diventano utilizzatrici;
- *Task service*. Piattaforme che implementano singole funzionalità trasversali alla realizzazione di procedimenti amministrativi digitali (ad esempio l'autenticazione degli utenti attraverso SPID) che le PA integrano all'interno dei loro sistemi;
- *Data service*. Piattaforme che assicurano l'accesso a fonti di dati validati (ad esempio l'utilizzo dei dati anagrafici assicurato da ANPR) di cui le PA necessitano per dare seguito alle proprie funzioni istituzionali.

Sulla base di tali evidenze, l'Ateneo intende promuovere processi di adozione di piattaforme che possano supportare processi di reclutamento, di stipula di contratti e di convenzioni e di gestione di help desk unico, di gestione sedute organi e delibere. Nell'ambito del e-recruitment l'Ateneo, sulla base di una specifica attività avviata nel corso del 2019, finalizzata alla razionalizzazione delle attività associate alla gestione delle procedure concorsuali, è stata adottata la Piattaforma Integrata Concorsi Atenei (PICA), la quale consente di:

- automatizzare i processi amministrativi;
- dematerializzare l'iter concorsuale eliminando il cartaceo;
- protocollare e facilitare la conservazione digitale degli atti;
- validare i dati inseriti dai candidate;
- consentire l'applicazione della firma digitale;
- integrare servizi di terze parti, come SPID, PagoPA e sistemi di gestione dei flussi.

### 3.4 SICUREZZA INFORMATICA E MODALITÀ ATTUATIVE DEL LAVORO AGILE

L'incremento dei servizi digitali erogati dalla Pubblica Amministrazione produce come naturale conseguenza l'innalzamento del rischio derivante dalle vulnerabilità software dei sistemi operativi, delle molteplici applicazioni presenti nelle infrastrutture ICT e delle piattaforme hardware presenti nei Data Center. La moltiplicazione degli attacchi informatici, con particolare riferimento a quelli provenienti dal Cyberspace, ha assunto la connotazione di un problema cruciale per le aziende operanti in settori e con dimensioni diverse. La dimensione della sicurezza delle informazioni, caratterizzata *“dalla salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite da un'organizzazione”*, è riconducibile prioritariamente a quella degli attacchi informatici, ma può riguardare anche altri fenomeni, come quello delle calamità naturali o della mancanza di una *“cultura della sicurezza”* da parte del personale operante nell'organizzazione. Più specificatamente, con il termine di *“sistema di sicurezza delle informazioni”* si vuole intendere *“l'insieme di*

*prodotti, servizi, regole organizzative e comportamenti individuali finalizzati alla protezione dei sistemi informatici di un'azienda.*” Per la Pubblica Amministrazione l'attività di contrasto alle minacce cibernetiche ha assunto un'importanza fondamentale, soprattutto per quanto concerne la disponibilità, l'integrità e la riservatezza delle informazioni possedute, ma in particolare per garantire la fiducia nei servizi digitali erogati dalla PA. Tra gli obiettivi del Piano Triennale è possibile rilevare il punto sulla *Cyber Security Awareness*, dal quale si evince che dalla consapevolezza del rischio ciberneticò possono derivare opportune azioni organizzative e proattive utili alla mitigazione dei pericoli derivanti da possibili attacchi informatici. Sulla base di tale evidenza, l'Ateneo si propone di definire momenti di formazione e campagne informative finalizzate alla diffusione della cultura della sicurezza informatica tra il personale. Contestualmente si propone di adottare strumenti specifici (come ad esempio Gophish<sup>3</sup>) che possano permettere, ad esempio, la simulazione e il monitoraggio di campagne di phishing, una tecnica efficace per incrementare il livello di consapevolezza sui rischi cyber legati al phishing. Va evidenziato che l'Agenzia per l'Italia Digitale ha promosso uno specifico progetto che si pone l'obiettivo di supportare tutte le Pubbliche Amministrazioni per l'adozione di una metodologia di Cyber Risk Management<sup>4</sup> sviluppata nell'ambito del Piano Triennale per l'informatica nella Pubblica Amministrazione. A tal fine, l'AgID ha realizzato un tool di valutazione e trattamento del rischio cyber che consente ad ogni PA di effettuare le operazioni di self-assessment, i piani di trattamento e il monitoraggio delle iniziative volte a ridurre il livello di rischio informatico. L'Ateneo intende quindi adottare tale strumento per incrementare al fine di effettuare un self-assessment di sicurezza informatica, migliorare la consapevolezza sulle materie di cybersecurity e valutare le vulnerabilità e il livello di esposizione al rischio cyber. Sulla base delle indicazioni del Governo, che tendono ad incentivare l'adozione del lavoro agile o Smart Working nelle PA e l'utilizzo da parte del dipendente pubblico di appositi dispositivi tecnologici utili allo svolgimento delle prestazioni lavorative, le amministrazioni pubbliche devono definire e adottare specifici livelli di sicurezza e protezione della rete, rafforzando la consapevolezza dei dipendenti sui pericoli derivanti dall'utilizzo di dispositivi personali e applicativi insicuri. Sulla base di questa evidenza, l'Ateneo si adopererà per innalzare la consapevolezza del rischio informatico legato al lavoro agile tramite azioni finalizzate alla formazione, alla realizzazione di informative e di apposite soluzioni tecnologiche per garantire la sicurezza dei lavoratori in Smart Working.

### **3.5 STUDIO DELLA POSSIBILITA' DI ADOTTARE PIATTAFORME DI INTELLIGENZA ARTIFICIALE (IA)**

Il 26 settembre 2023 Microsoft ha rilasciato l'aggiornamento di Windows 11 più interessante degli ultimi anni, con, tra gli altri, diversi aggiornamenti legati all'intelligenza artificiale come strumenti IA di disegno per Paint, strumenti di estrazione del testo (di tipo IA), ma soprattutto di un nuovo prodotto verticalizzato sull'utilizzo dell'intelligenza artificiale: Windows Copilot. Introdotto come preview, Copilot è un assistente AI creato da Microsoft e alimentato dalla sua tecnologia di modelli linguistici di grandi dimensioni, e che si integra con Windows tramite una specifica barra laterale intelligente. Lo strumento sostituisce l'assistente "Cortana" e migliora l'applicazione "Bing Chat" a livello di proattività. Oltre a essere integrato in Windows 11, Copilot è richiamabile da qualsiasi applicazione e funziona anche all'interno delle stesse, come nel caso di Edge o della suite di produttività Microsoft 365, che fa ampio uso dello strumento. Il 1 dicembre 2023, con il rilascio del secondo aggiornamento cumulativo di novembre, è iniziato il rilascio di Copilot anche su Windows 10. Copilot si pone come una chatbot generativa, che consente di evitare di attivare ChatGPT o strumenti simili. Inoltre può consentire di agevolare gli operatori sul piano lavorativo, mediante la fruizione di una serie di utilities di particolare rilevanza (dettare una email, leggere un testo da uno screenshot, effettuare automaticamente una chiamata su Skype, correggere automaticamente una relazione, etc.). Copilot, grazie alle ampissime funzionalità di cui dispone, può essere ulteriormente utilizzato in termini di raccolta di specifiche informazioni, grazie ai plugin di cui dispone e che possono consentire di leggere automaticamente i PDF, effettuare calcoli e molto altro, proprio come avviene per ChatGPT Plus. Sulla base dello studio condotto nel periodo di riferimento della presente relazione, è stato possibile verificare l'esistenza di collaborazioni in atto con altre applicazioni e strutture operanti nel settore, come OpenTable,

Wolfram Alpha, Expedia, Instacart, Kayak, Klarna, Redfin, TripAdvisor e Zillow. Ciò consentirà a Copilot di fornire informazioni specifiche per una serie di contesti, oltre ai consigli contestuali basati sulla conversazione. La possibilità di recuperare informazioni sarà invece particolarmente importante per le organizzazioni, che potranno incorporare il chatbot nella loro rete aziendale perché possa attingere ai dati ed effettuare calcoli o avviare operazioni su richiesta. E tutto questo è disponibile in Windows 11, ora, grazie all'aggiornamento facoltativo Moment 4 (KB5030310) tramite Windows Update. Come già evidenziato, Copilot è integrato in Microsoft 365 e fornisce contenuti pertinenti che consentono di risparmiare tempo prezioso, riconoscendo i modelli di lavoro e automatizzando le attività ripetitive, come la pianificazione di riunioni, l'organizzazione di file e la creazione di report. A tal proposito, in Word, Copilot può essere usato alla stregua di ChatGPT, ovvero per scrivere contenuti, modificare o correggere uno scritto, fornire consigli grammaticali o stilistici, sia dal punto di vista lessicale che della sintassi. Può essere usato come fonte di ispirazione o come editor, come compagno per superare il blocco dello scrittore o per creare la struttura di un racconto. In Excel, Copilot può servire per analizzare un database per cercare tendenze o modelli non immediatamente ovvi, o per visualizzare i dati nei modi più chiari per trasmettere un messaggio. In PowerPoint, Copilot può creare intere presentazioni per l'utente a partire da un semplice prompt. In Microsoft Outlook, Copilot può aiutare gli utenti a gestire le loro caselle di posta per ordinare meglio le email o scandagliarle per trovare informazioni non accessibili attraverso uno strumento tradizionale. In Teams, Copilot può riassumere intere riunioni e chat, nel caso di assenza dell'utente o di ritardo nella partecipazione. Microsoft 365 Copilot, è disponibile sul mercato dal 1° novembre 2023 insieme Microsoft 365 Chat, un nuovo assistente IA in grado di rispondere alle domande, gestire tutti i dati personali dell'utente fra cui email, appuntamenti, chat, documenti e molto altro. Inoltre Microsoft ha lanciato Copilot Lab, uno strumento di aiuto integrato in Microsoft 365 Copilot per sfruttare al meglio le funzioni IA. Sulla base dell'analisi condotta in Ateneo e dell'evidenza dell'utilizzo da parte dell'università delle applicazioni Microsoft 365, a partire dal primo trimestre 2024, grazie all'apporto di alcuni Settori della Divisione 9 – Informatica, sarà condotto uno studio di fattibilità sulla possibile sperimentazione dell'applicazione Copilot all'interno dell'Ateneo.

#### **Punto OB.2.1 (Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese)**

**Periodo: 2024-2025**

**Azioni dell'Ente: L'Ateneo aderisce alla Misura 1.3.1. "Piattaforma Digitale Nazionale Dati" Università e AFAM pubblici (Luglio 2023) del Dipartimento per la Trasformazione Digitale.** Con riferimento all'avviso Missione 1, Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa NextGenerationEU, nell'ambito dell'Investimento 1.3. "Dati e interoperabilità", parte della Misura 1.3.1. "Piattaforma Digitale Nazionale Dati" è stato condotto uno studio sulla possibile adesione dell'Ateneo al progetto in questione. Va evidenziato che la Milestone ed i Target europei previsti per la Misura 1.3.1 sono i seguenti:

- a) Milestone M1C1-4 conseguita a ottobre 2022: la piattaforma deve consentire agli enti/agenzie di:
  - a. pubblicare le rispettive interfacce per programmi applicativi (API) sul catalogo API della piattaforma;
  - b. redigere e firmare accordi sull'interoperabilità digitale attraverso la piattaforma;
  - c. autenticare e autorizzare l'accesso alle API utilizzando le funzionalità della piattaforma;
  - d. convalidare e valutare la conformità al quadro nazionale in materia di interoperabilità.
- b) Target M1C1-18 da conseguirsi entro dicembre 2024: l'obiettivo consiste nel raggiungimento di almeno 400 interfacce per programmi applicativi API (Application Programming Interface) pubblicate nel catalogo API e integrate con PDND. Le API pubblicate devono avere un impatto sui seguenti settori:

- a. al 31 dicembre 2023: servizi prioritari di sicurezza sociale e conformità fiscale. compresi i principali registri nazionali (come il registro anagrafico e il registro della pubblica amministrazione);
  - b. entro il 31 dicembre 2024: i servizi rimanenti di sicurezza sociale e conformità fiscale. Ciascuna attuazione e documentazione di API deve essere conforme alle norme nazionali di interoperabilità e sostenere il quadro della National Digital Data Platform; la piattaforma di cui sopra fornisce funzionalità per valutare tale conformità.
- c) Target M1C1-27 da conseguirsi entro giugno 2026: L'obiettivo consiste nel raggiungimento di almeno ulteriori 600 interfacce per programmi applicativi API (Application Programming Interface) pubblicate nel catalogo (per un totale di 1000). Le API pubblicate devono avere un impatto sui seguenti settori:
- i. entro il 31 dicembre 2025: procedure pubbliche quali assunzioni, pensionamento, iscrizione a scuole e università (come l'Anagrafe Nazionale Studenti e dei laureati e il Pubblico registro automobilistico);
  - ii. entro il 30 giugno 2026: welfare, gestione dei servizi di appalto, sistema informativo nazionale per i dati medici e le emergenze sanitarie – ad es. i registri dei pazienti e dei medici. Ciascuna attuazione e documentazione di API deve essere conforme alle norme nazionali di interoperabilità e sostenere il quadro della National Digital Data Platform; la piattaforma di cui sopra fornisce funzionalità per valutare tale conformità. L'importo del finanziamento concedibile ai Soggetti attuatori di cui all'art. 5 è individuato, ai sensi dell'art. 53 par. 1. lett. c) e par.3 lett.a) punto i) del Reg. UE 1060/2021, in un importo forfettario (lump sum) determinato in funzione della dimensione delle Università e degli AFAM pubblici, suddivisi in fasce di appartenenza e dalla erogazione di un numero di API come definito nell'Allegato 2 (*di seguito riportato*) del presente Avviso. Il finanziamento, nella misura dell'importo forfettario, sarà erogato in un'unica soluzione a seguito del perfezionamento delle attività oggetto del finanziamento, come disposto all'art. 13 del presente Avviso. Va evidenziato che il Piano Nazionale di Ripresa e Resilienza (PNRR) valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio, notificata all'Italia dal Segretariato generale del Consiglio con nota LT 161/21, del 14 luglio 2021 e, in particolare, la Missione 1 – Componente 1 – Misura 1.3.1 "*Piattaforma Digitale Nazionale Dati*" attribuisce una dotazione complessiva di euro 556.000.000,00.

Sulla base dello studio condotto dallo scrivente e dell'evidenza della possibilità da parte dell'Ateneo di accedere al progetto e al relativo finanziamento, in data 27.10.2023 è stato sottoscritto digitalmente dal Rettore dell'Ateneo, Prof. Liborio Stuppia, il documento di adesione al progetto e successivamente inserito sulla piattaforma online PA digitale 2026.

## Allegato 2 – Definizione del Servizio e modalità di integrazione

<b>1</b>	<b>Sommario</b>	
<b>2</b>	<b>Ambito di applicazione</b>	<b>2</b>
<b>3</b>	<b>Definizione del Catalogo API</b>	<b>2</b>
<b>4</b>	<b>Obiettivi di erogazione di servizi</b>	<b>3</b>
4.1	Erogazione: Specifiche tecniche	3
4.2	Erogazione: Numero API e modalità	5
4.2.1	Fascia 1 "Micro": Università e AFAM pubblici con numero di studenti tra 0 e 1000	6
4.2.2	Fascia 2 "Piccoli": Università e AFAM pubblici con numero di studenti tra 1001 e 10000	6
4.2.3	Fascia 3 "Medi": Università e AFAM pubblici con numero di studenti tra 10001 e 20000	6
4.2.4	Fascia 4 "Grandi": Università e AFAM pubblici con numero di studenti tra 20001 e 40000	6
4.2.5	Fascia 5 "Mega": Università e AFAM pubblici con numero di studenti superiore ai 40000	6
<b>5</b>	<b>Pattern di sicurezza</b>	<b>7</b>
<b>6</b>	<b>Le modalità di onboarding ed erogazione dei servizi</b>	<b>7</b>
6.1	Processo di onboarding	7
6.2	Sviluppo dei servizi e delle relative API	7
6.3	Pubblicazioni API su Piattaforma PDND di Test	8
6.4	Pubblicazioni API su Piattaforma PDND di Produzione	8
6.5	Conclusione del processo di integrazione e di attivazione dei servizi	9
<b>7</b>	<b>Listino di riferimento</b>	<b>10</b>

## 2 Ambito di applicazione

Il presente documento descrive le modalità, il servizio e il processo di integrazione dei servizi all'interno dell'investimento M1C1-1.3.1 - Piattaforma Digitale Nazionale Dati ("PDND"), in favore delle Università pubbliche e degli Istituti di Alta formazione artistica, musicale e coreutica (di seguito AFAM) pubblici.

La PDND è la piattaforma definita all'articolo 50-ter, comma 2 del Decreto legislativo 7 marzo 2005, n. 82 cui i soggetti di cui all'articolo 2, comma 2, del CAD si avvalgono al fine di favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto per finalità istituzionali nelle banche dati a loro riferibili nonché la condivisione dei dati con i soggetti che hanno diritto di accedervi in attuazione dell'articolo 50 del CAD per la semplificazione degli adempimenti dei cittadini e delle imprese. I processi di accreditamento, identificazione e autorizzazione; le modalità con cui i soggetti interessati danno seguito alle reciproche transazioni; le modalità di raccolta e conservazione delle informazioni relative agli accessi e altre transazioni effettuate sono determinate dalle "Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati", adottate da AgID con determinazione n. 679 del 15 dicembre 2021 e modificate con determinazione n. 26 del 3 febbraio 2022.

PDND favorisce l'interoperabilità dei sistemi informativi e delle basi di dati delle Pubbliche Amministrazioni e dei gestori di servizi pubblici. Il livello di interoperabilità proposto da PDND è attuabile mediante l'accREDITamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa, nonché la raccolta e la conservazione delle informazioni relative agli accessi e alle transazioni effettuate per il suo tramite.

## 3 Definizione del Catalogo API

In riferimento al paragrafo 4.9 delle *Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati* adottate da AgID, un'API è definita come: "Un insieme di procedure, funzionalità e/o operazioni disponibili al programmatore, di solito raggruppate a formare un insieme di strumenti specifici per l'espletamento di un determinato compito".

La definizione di **e-service** si trova, invece, nelle *Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni* adottate da AgID. In breve, si tratta di un servizio digitale realizzato da un soggetto aderente alla PDND, attraverso l'implementazione delle necessarie API conformi alle *Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni* e alle *Linee Guida Tecnologie e*

standard per assicurare la sicurezza dell'interoperabilità tramite API dei sistemi informatici, per assicurare ai soggetti aderenti alla PDND l'accesso ai dati e/o l'integrazione di processi.

PDND realizza la componente unica e centralizzata prevista dalle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni, che assicura agli enti Erogatori la registrazione e la pubblicazione dei propri e-service, agli enti Fruttori la consultazione degli e-service pubblicati (Catalogo API).

## 4 Obiettivi di erogazione di servizi

L'obiettivo del presente avviso è l'erogazione di API nel Catalogo API PDND da parte delle Università pubbliche e degli AFAM pubblici.

Nel quadro del progetto di interoperabilità, quindi, un'API è un'interfaccia applicativa che:

- è identificata nel Catalogo API dalla sua documentazione secondo gli standard previsti nel *Modello di interoperabilità* descritto nelle linee guida indicate al paragrafo B;
- è identificata nel catalogo API dal riferimento del suo punto di erogazione principale (server URL di produzione);
- rispetta le cornici di sicurezza indicate al paragrafo D;
- consente di effettuare tutte le operazioni associate alla procedura relativa.

In conformità alle *Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni* sarà consentito l'erogazione delle API nella modalità HTTP REST. Queste dovranno essere pubblicate attraverso un descrittore *OpenAPI 3* che dovrà contenere il dettaglio di tutti gli endpoint che lo compongono. Per ogni endpoint andranno indicati tutti gli *HTTP methods* implementati. Il formato del descrittore dovrà essere JSON o YAML.

### 4.1 Erogazione: Specifiche tecniche

Per il presente avviso è prevista l'erogazione delle seguenti 9 API secondo le modalità del paragrafo 4.2:

	API ID	Titolo	Descrizione
API 1	IFS01	Offerta formativa	Acquisizione dei dati dei corsi attivi ed offerti da un Istituto in un dato anno accademico
API 2	IFS02	Iscrizioni studente	Acquisizione dei dati di dettaglio delle iscrizioni di uno studente/ex-studente in formato nazionale.
			Acquisizione dei dati di dettaglio delle iscrizioni di uno studente/ex-studente in formato transfrontaliero.

			Acquisizione dei dati di dettaglio delle iscrizioni e degli esami sostenuti con voto (transcript) di uno studente/ex-studente in formato transfrontaliero.
API 3	IFS03	Titoli studente	Acquisizione dei titoli conseguiti nell'istituto da uno studente/ex-studente in formato nazionale
			Acquisizione del Diploma Supplement semplificato (senza voti degli esami) in formato transfrontaliero.
			Acquisizione del Diploma Supplement in formato transfrontaliero.
API 4	IFS04	Rettifica iscrizioni studente	<p>Permette di richiedere la rettifica dei dati di un'iscrizione o una iscrizione mancante per uno studente/ex-studente.</p> <p>Funzionalità ulteriori:</p> <ul style="list-style-type: none"> <li>- Lista degli attributi modificabili</li> <li>- Possibilità di monitorare lo stato della richiesta di rettifica</li> </ul>
API 5	IFS05	Rettifica titoli studente	<p>Vuole richiedere la rettifica dei dati di un titolo conseguito o mancante di uno studente/ex-studente.</p> <p>Funzionalità ulteriori:</p> <ul style="list-style-type: none"> <li>- Lista degli attributi modificabili</li> <li>- Possibilità di monitorare lo stato della richiesta di rettifica</li> </ul>
API 6	IFS06	Elenco Variazioni Iscrizioni	Acquisizione della lista degli studenti che hanno subito un cambio di stato alla relativa iscrizione tra un istante t0 e uno t1 (ad es. t0 = 1 gennaio 2019 e t1 = 31 dicembre 2019 per richiedere i dati relativi all'anno solare 2019)
API 7	IFS07	Elenco variazione titoli	Acquisizione della lista degli studenti che hanno subito un cambio di stato ai relativi titoli conseguiti tra un istante t0 e uno t1 (ad es. t0 = 1 gennaio 2019 e t1 = 31 dicembre 2019 per richiedere i dati relativi all'anno solare 2019)
API 8	IFS08	Iscritti per fasce ISEE	Acquisizione del numero di studenti per fasce ISEE in un anno accademico, per facoltà e per intero Istituto

API 9	IFS09	Iscritti a un corso per anno	Acquisizione del numero di studenti iscritti a una facoltà o ad un corso specifico per anno accademico
-------	-------	------------------------------	--

Tabella 1 - Tabella di descrizione delle 9 API da erogare da parte delle Università e AFAM, in base alla fascia di appartenenza

Si precisa che la API 2 (ID IFS02) e la API 3 (ID IFS03), elencate nella tabella 1, includono le tre sottocategorie di dati dettagliati nella colonna "Descrizione", che dovranno essere erogati da parte delle Università e AFAM affinché possano essere eleggibili per il finanziamento.

Tutti i dettagli relativi alle API e agli endpoint saranno disponibili tra le *Implementazioni* nella sezione *Risorse* della pagina di Developers Italia <https://developers.italia.it/it/pdnd/#risorse> o in alternativa sul main repository <https://github.com/italia/api-padigitale2026-misura1.3.1-uni-afam>. Saranno lì messi a disposizione tutti i descrittori delle API che le Università e gli AFAM dovranno implementare e pubblicare.

#### 4.2 Erogazione: Numero API e modalità

Il presente bando prevede dei requisiti diversi per le Università e per gli AFAM pubblici che potranno aderire all'avviso sulla base del numero di iscritti. Per la suddivisione degli Istituti è stata utilizzata la Classificazione CENSIS 2022/2023 <sup>(1)</sup> secondo cui gli Istituti vengono divisi in cinque fasce sulla base del numero di studenti iscritti, come indicato nei paragrafi che seguono. Il dimensionamento degli interventi dipende dal **livello di complessità** dei sistemi attualmente in uso presso le Amministrazioni oltre che dalla numerosità delle API che ciascuna delle Amministrazioni integrerà su PDND. Sono state ipotizzate 3 tipologie di scenari basati sulla complessità dei Sistemi Informativi degli Enti che erogheranno i servizi:

- API semplice
- API media
- API complessa

I Criteri di Complessità possono essere associati agli Istituti di Formazione, Atenei e AFAM, tenendo in considerazione vari fattori:

- Un Istituto con più studenti avrà un numero maggiore di Facoltà e di Corsi di laurea; quindi, i dati possono essere collezionati da più fonti rendendo più complesso il reperimento degli stessi
- Un Istituto con più studenti può avere più sistemi gestionali che devono essere messi in comunicazione per organizzare una risposta completa all'API erogata

<sup>1</sup> [https://www.censis.it/sites/default/files/downloads/Classifica%20Censis%20delle%20Universita%20italiane%202022\\_2023.pdf](https://www.censis.it/sites/default/files/downloads/Classifica%20Censis%20delle%20Universita%20italiane%202022_2023.pdf)

- A parità di API da erogare, un Istituto con più studenti avrà più dati da raccogliere ed organizzare per strutturare la risposta all'interrogazione

Il fattore con il peso maggiore per la determinazione della fascia di complessità è quindi la quantità di dati contenuti nella risposta alle API più che al numero di API da erogare.

#### 4.2.1 Fascia 1 "Micro": Università e AFAM pubblici con numero di studenti tra 0 e 1000

La Fascia 1, "Micro", è stata inserita per segmentare ulteriormente la fascia "Piccoli" previsti dal CENSIS in modo da differenziare gli Istituti fino a 1000 studenti. Per l'erogazione del contributo le Università e gli AFAM pubblici classificati come "Micro" dovranno erogare le **7 API** che sono identificate con gli API ID che vanno da *IFS01* a *IFS07* come indicato al paragrafo 4.1. La complessità delle API da erogare da parte della Fascia 1 sarà identificata come bassa.

#### 4.2.2 Fascia 2 "Piccoli": Università e AFAM pubblici con numero di studenti tra 1001 e 10000

Per l'erogazione del contributo le Università e gli AFAM pubblici classificati come "Piccoli" dovranno erogare le **8 API** che sono identificate con gli API ID che vanno da *IFS01* a *IFS08* come indicato al paragrafo 4.1. La complessità delle API da erogare da parte della Fascia 2 sarà identificata come bassa.

#### 4.2.3 Fascia 3 "Medi": Università e AFAM pubblici con numero di studenti tra 10001 e 20000

Per l'erogazione del contributo le Università e gli AFAM pubblici classificati come "Medi" dovranno erogare le **8 API** che sono identificate con gli API ID che vanno da *IFS01* a *IFS08* come indicato al paragrafo 4.1. La complessità delle API da erogare da parte della Fascia 3 sarà identificata come media.

#### 4.2.4 Fascia 4 "Grandi": Università e AFAM pubblici con numero di studenti tra 20001 e 40000

Per l'erogazione del contributo le Università e gli AFAM pubblici classificati come "Grandi" dovranno erogare le **9 API** che sono identificate con gli API ID che vanno da *IFS01* a *IFS09* come indicato al paragrafo 4.1. La complessità delle API da erogare da parte della Fascia 4 sarà identificata come media.

#### 4.2.5 Fascia 5 “Mega”: Università e AFAM pubblici con numero di studenti superiore ai 40000

Per l'erogazione del contributo le Università e gli AFAM pubblici classificati come “Mega” dovranno erogare le **9 API** che sono identificate con gli API ID che vanno da *IFS01* a *IFS09* come indicato al paragrafo 4.1. La complessità delle API da erogare da parte della Fascia 5 sarà identificata come alta.

## 5 Pattern di sicurezza

Per l'erogazione dei servizi di cui al paragrafo 4, le Università e gli AFAM dovranno usare il solo token emesso da PDND senza la richiesta di ulteriori certificati di sicurezza, pattern di sicurezza descritto nelle *Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni (Modl)*<sup>2</sup> (allegato 2 *Pattern di Sicurezza*)<sup>3</sup>.

L'utilizzo di questo pattern dovrà essere espressamente indicato nella documentazione a corredo di ogni e-service.

L'utilizzo di altri pattern di sicurezza, se pur previsti dal Modl, non potranno essere ritenuti validi ai fini dell'asseverazione di questo avviso.

## 6 Le modalità di onboarding ed erogazione dei servizi

Di seguito, si dà evidenza del processo formale e tecnico per l'integrazione di API su PDND.

### 6.1 Processo di onboarding

Le attività da porre in essere per l'erogazione di API da parte delle Università e AFAM pubblici su PDND sono le seguenti:

- Essere regolarmente iscritti sull'Indice delle Pubbliche Amministrazioni (IPA) con dati aggiornati
- Completamento della procedura di adesione sul portale Self Care messo a disposizione da PagoPA S.p.A. o altra modalità individuata dalla PagoPA S.p.A.:
  - Selezione dell'ente per cui si intende aderire;
  - Indicazione del Rappresentante Legale e dei Referenti amministrativo e tecnico;

<sup>2</sup> [https://www.agid.gov.it/sites/default/files/repository\\_files/linee\\_guida\\_interoperabilit\\_tecnica\\_pa.pdf](https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf)

<sup>3</sup> Per accedere all'allegato del pdf, scaricare il pdf delle Linee Guida ed aprirlo con un visualizzatore pdf come ad esempio Adobe Acrobat che mostrerà gli allegati del pdf.

- Firma digitale dell'accordo di adesione da parte del rappresentante legale: l'accordo viene inviato sulla PEC dell'Istituto presente in IPA a valle della procedura svolta per l'adesione;
- Caricamento dell'accordo di adesione firmato al link di conferma ricevuto nella stessa PEC;

## 6.2 Sviluppo dei servizi e delle relative API

- Sviluppo dei servizi e delle relative API:
  - secondo le linee guida indicate nei paragrafi 2 e 3
  - in numero pari alle quantità indicate al paragrafo 4
  - con la cornice di sicurezza indicata al paragrafo 5

## 6.3 Pubblicazioni API su Piattaforma PDND di Test

- Una volta effettuato l'onboarding, eleggere le figure di riferimento di PDND come indicato nelle appendici delle *"Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati"*
- Effettuare il caricamento delle chiavi e dei certificati necessari alla comunicazione con PDND, come indicato nei manuali operativi
- Pubblicare le API corredate di:
  - attributi di accesso al servizio, come indicato nel manuale utente
  - documentazione tecnica (OAS yaml)
  - documentazione sui requisiti di sicurezza per l'accesso.
- Configurare le API con fruizione automatica da parte del Ministero dell'Università e della Ricerca (MUR)
- Effettuare attività di UAT in ambiente di Test;

## 6.4 Pubblicazioni API su Piattaforma PDND di Produzione

- Una volta superate le attività di Test nella piattaforma di Test, pubblicare le API in piattaforma di produzione ripercorrendo tutti i passi effettuati per la piattaforma di Test.

Le attività oggetto del corrente bando, di cui al paragrafo C del presente allegato, saranno considerate concluse con il completamento del percorso di pubblicazione sulla piattaforma di produzione di ciascuna API e dell'erogazione dei relativi servizi.

L'Università o l'AFAM che risponderà all'avviso assicurerà:

- la piena operatività dei servizi erogati, oggetto di questo avviso, almeno fino a dicembre 2026. Sarà possibile la verifica di fruizione a campione di API per testare la qualità e l'effettiva erogazione dei servizi;
- la configurazione dei servizi erogati con fruizione automatica da parte del Ministero dell'Università e della Ricerca (MUR).

All'atto dell'inizio delle attività l'Istituto otterrà da PagoPA S.p.A. la seguente documentazione:

- Manuale Operativo di Piattaforma Digitale Nazionale Dati;
- Specifiche tecniche per documentare le API fornite da Piattaforma Digitale Nazionale Dati, con inclusi i Sequence Diagram che ne dimostrano l'utilizzo;
- Materiale esplicativo addizionale: Q&A e video online su PDND;
- Presentazioni e white papers per lo sviluppo di API secondo il modello di interoperabilità;
- Modello di tracciamento dell'esecuzione dei test e dei risultati ottenuti.

La società si riserva di comunicare tempestivamente eventuali nuove modalità di onboarding e attivazione dei servizi, tramite apposita comunicazione ufficiale.

Le attività per il raggiungimento degli obiettivi del presente avviso possono essere svolte dalle Università/AFAM tramite il supporto di un Partner/Intermediario Tecnologico (se già contrattualizzato), o attraverso l'individuazione di un Partner/intermediario Tecnologico, per lo sviluppo di processi di reingegnerizzazione tali da garantire l'integrazione informatica con le soluzioni gestionali in uso presso l'Istituto e la piena rispondenza alle specifiche tecnico-operative previste per l'integrazione con PDND.

#### 6.5 Conclusione del processo di integrazione e di attivazione dei servizi

Le attività sopra menzionate dovranno essere eseguite nei seguenti termini:

- massimo 3 mesi (90 giorni) per la contrattualizzazione del fornitore dalla data di notifica del decreto di finanziamento;
- massimo 6 mesi (180 giorni) per l'integrazione e attivazione dei servizi, a partire dalla data di contrattualizzazione del fornitore.

Il cronoprogramma è unico per tutte e cinque le fasce di Università e AFAM.

Il processo di integrazione ed erogazione dei servizi si intende concluso con esito positivo nel momento in cui vengono pubblicate ed attivate dall'Università o AFAM le API nel Catalogo API della PDND. L'evidenza del completamento di tali attività sarà riscontrabile interrogando appositi servizi della PDND che restituiranno, per ogni Istituto, il nome ed il numero di API presenti nel Catalogo.

***Resta inteso che l'erogazione del contributo per PDND è prevista solo ed esclusivamente nel caso in cui l'ente abbia rispettato quanto indicato in fase di adesione, ossia abbia completato il processo di onboarding ed erogazione del numero di servizi come indicato nel paragrafo C.***

***Elemento vincolante al finanziamento è la configurazione dei servizi con fruizione automatica per il Ministero dell'Università e della Ricerca (MUR), come esplicitato nel paragrafo E.***

Inoltre, si precisa che i servizi messi a disposizione dovranno rimanere attivi ed essere effettivamente utilizzati e movimentati per un periodo di tempo di almeno 5 anni dalla data di pubblicazione. Un'eventuale verifica negativa comporterà la revoca del finanziamento.

## 7 Listino di riferimento

L'importo del contributo, in forma forfettaria, sarà riconosciuto al Soggetto Attuatore solo a seguito del conseguimento del risultato atteso, così come dettagliato nei paragrafi C e D di questo allegato.

Gli importi del contributo sono così definiti:

(A)	(B)	(C)	(D)
Fascia	Studenti	# API	Lump Sum per Istituto
1	$\leq 1000$	7	71.885,45 €
2	$1000 < \text{studenti} \leq 10000$	8	82.154,80 €
3	$10000 < \text{studenti} \leq 20000$	8	321.958,00 €
4	$20000 < \text{studenti} \leq 40000$	9	362.202,75 €
5	$> 40000$	9	704.421,90 €

Tabella 2 - Tabella di individuazione dell'importo forfettario riconoscibile per fascia di Istituto Universitario

Dove le varie colonne indicano:

- A. Fascia di appartenenza dell'Istituto
- B. Numero di studenti della fascia
- C. Numero minimo di API da attivare per il riconoscimento dell'importo forfettario
- D. Importo Lump sum riconosciuto per ogni istituto della fascia